Кевин Митник

«ИСКУССТВО БЫТЬ НЕВИДИМЫМ»

Посвящается моей любимой маме, *Шелли Джаффе*, и моей бабушке, *Ребе Вартанян*

Предисловие *Микко Хиппонена*

Несколько месяцев назад я встретил старого друга, которого не видел со старших классов школы. Мы зашли выпить кофе и поговорить о том, чем каждый из нас занимался последние пару десятилетий. Он рассказал мне, что занимается продажей и техническим обслуживанием различной современной медицинской техники, а я поведал, что последние двадцать пять лет моя работа связана с интернет-безопасностью и защитой персональных данных. Друг даже прищелкнул языком, когда услышал про защиту персональных данных. «Звучит очень интересно и здорово, — сказал он, — но меня эта тема не слишком волнует. Ведь я не преступник и не делаю ничего плохого. Ну и что, если кто-нибудь узнает, чем я занимаюсь в Интернете».

Когда я слушал своего старого друга и его рассуждения о том, почему конфиденциальность для него не важна, мне стало грустно. Грустно оттого, что я слышу подобные слова очень часто. Я слышал их от людей, которые считают, что им нечего скрывать. От людей, которые уверены, что только преступникам нужно беспокоиться о своей защите. От людей, которые думают, что только террористы используют шифрование. От людей, которые убеждены, что нам не нужно отстаивать свои права. Но нам нужно отстаивать свои права. А безопасность персональных данных — это не просто наше законное право, это общечеловеческое право. По сути, право на неприкосновенность личной жизни считается одним из фундаментальных человеческих прав с 1948 года, когда Организация Объединенных Наций приняла Всеобщую декларацию прав человека.

Если наше право на безопасность персональных данных нуждалось в защите уже в 1948 году, в наше время такая необходимость еще сильнее. В конце концов, мы — первое поколение в человеческой истории, за которым можно следить на столь высоком уровне. За нашей жизнью можно наблюдать с помощью цифровых технологий. Тем или иным образом можно выяснить содержание практически каждого нашего разговора. Более того, мы постоянно носим с собой маленькие устройства слежения — просто мы их таковыми не считаем, а называем смартфонами.

Благодаря интернет-слежке за пользователями в Интернете можно узнать, какие книги мы покупаем и какие статьи читаем, — даже какие части прочитанных статей вызвали у нас наибольший интерес. Можно посмотреть, где и с кем путешествуем. Благодаря интернет-слежке можно понять, больны мы или здоровы, грустно нам или весело, аскетичны мы или сексуально озабочены. Почти вся слежка в Интернете направлена на то, чтобы заработать деньги на полученных данных. Компании, которые предлагают людям бесплатные услуги, каким-то образом умудряются заработать на этих бесплатных услугах миллиарды долларов — прекрасная иллюстрация того, насколько выгодно собирать большие объемы данных о пользователях Интернета. Однако существует и более прицельная слежка: со стороны спецслужб, иностранных и внутренних.

Благодаря цифровым технологиям правительство может собирать данные массово. Но и мы тоже можем защищать себя гораздо эффективнее, чем раньше. К нашим услугам такие средства и способы защиты, как шифрование, надежные методы хранения данных и соблюдение основных принципов безопасности операций (OPSEC). Нам просто нужно узнать, как правильно это делать.

Что же, ключ к этим знаниям здесь, в ваших руках. Я безмерно рад, что Кевин нашел время и поделился своим опытом в том, что касается искусства быть невидимым. В конце концов, он кое-что в этом понимает. Это великолепное пособие. Читайте, и пусть полученные знания пойдут вам во благо. Защищайте себя, защищайте свои права.

Возвращаясь к кофейне, когда я выпил кофе с другом, наши пути разошлись. Я пожелал ему всего наилучшего, но иногда до сих пор вспоминаю его слова: «Ну и что, если кто-нибудь узнает, чем я занимаюсь в Интернете».

Может быть, тебе и нечего скрывать, мой друг. Но тебе есть что защищать.

Микко Хиппонен *— главный специалист по безопасности в компании F-Secure. Он единственный человек на Земле, который выступал сразу на двух конференциях — DEF CON и TED.*

Введение

ПРИШЛО ВРЕМЯ ИСЧЕЗНУТЬ

Спустя почти два года после того, как Эдвард Джозеф Сноуден, сотрудник консалтинговой компании Booz Allen Hamilton, обнародовал первую порцию секретных материалов Агентства национальной безопасности США (АНБ), Джон Оливер, комик с телеканала HBO, в одном из выпусков своей передачи, посвященном неприкосновенности частной жизни и тотальному контролю, опрашивал случайных прохожих на Таймс-сквер в Нью-Йорке. Его вопросы были простыми и четкими. Кто такой Эдвард Сноуден? Что он сделал?

В вышедших в эфир фрагментах интервью никто не знал ответы на эти вопросы. Даже если кому-то имя казалось знакомым, человек не мог ответить, что именно (и зачем) Сноуден сделал. Поступив на работу в Агентство национальной безопасности, Эдвард Сноуден скачал миллионы секретных документов, которые он впоследствии передал репортерам, чтобы те сделали их достоянием мировой общественности. Оливер мог бы завершить этот выпуск программы на пессимистичной ноте — несмотря на то что эта история уже несколько лет мелькает в новостях, никому, казалось бы, нет никакого дела до внутреннего шпионажа со стороны государства, — но комик решил поступить иначе. Вместо этого он полетел в Россию, куда перебрался опальный Сноуден, и взял интервью у него лично.

Почему мы с видимым безразличием относимся к тому, что правительственное агентство записывает наши телефонные переговоры, просматривает наши электронные письма и даже текстовые сообщения? Вероятно, причина в том, что АНБ в большинстве случаев не влияет на жизнь практически никого из нас, по крайней мере так, чтобы это было заметно, т. е. не делает ничего, что мы бы *ощутили*.

Первый вопрос, который Оливер задал в Москве Сноудену, звучал следующим образом: «Чего вы пытались добиться?» Сноуден ответил, что хотел продемонстрировать миру, чего может добиться АНБ, собирая данные практически о каждом. Когда Оливер показал ему интервью, снятые на Таймс-сквер, в которых прохожие один за другим говорили, что не знают, кто такой Сноуден, тот ответил: «Что ж, нельзя донести информацию до каждого».

Почему мы так несведущи во всем, что касается неприкосновенности частной жизни, о которой говорят и Сноуден, и многие другие? Почему мы с видимым

безразличием относимся к тому, что правительственное агентство записывает наши телефонные переговоры, просматривает наши электронные письма и даже текстовые сообщения? Вероятно, причина в том, что АНБ в большинстве случаев не влияет на жизнь практически никого из нас, по крайней мере так, чтобы это было заметно, т. е. не делает ничего, что мы бы *ощутили*.

Но как Оливер также выяснил на Таймс-сквер в тот день, американцам все же важна неприкосновенность частной жизни, когда дело касается их дома. Помимо вопросов о Сноудене, Оливер задавал общие вопросы, касающиеся частной жизни. Например, когда он спросил, как они относятся к секретной (но выдуманной) правительственной программе, которая сохраняет пересылаемые через Интернет изображения обнаженных людей, жители Нью-Йорка также были единодушны в своих ответах — с той лишь разницей, что на этот раз они были категорически против. Один из опрошенных даже признался, что недавно отправил кому-то подобное фото.

Все, кто отвечал на вопросы тогда на Таймс-сквер, сошлись во мнении, что жители Соединенных Штатов должны иметь возможность конфиденциально обмениваться любыми материалами через Интернет — даже фотографиями пениса. Именно в этом и заключалась главная мысль Сноудена.

Оказалось, что выдуманная правительственная программа, сохраняющая фотографии обнаженных людей, гораздо ближе к реальности, чем вы можете себе представить. Как Сноуден объяснил Оливеру во время интервью, поскольку у таких компаний, как Google, серверы физически расположены по всему миру, даже простое сообщение (возможно, с элементами наготы) от мужа жене, находящейся в том же американском городе, может сначала оказаться на сервере за границей. Коль скоро эти данные покидают территорию США, пусть и всего на наносекунду, АНБ может, благодаря принятому в США «Патриотическому акту», перехватить и занести в архив это сообщение или электронное письмо (включая непристойную фотографию), поскольку технически оно попало на территорию США из заграничного источника. Мнение Сноудена: рядовые американцы попались в сети, раскинутые после событий 11 сентября, которые изначально были средством борьбы с терроризмом, а сейчас превратились в средство слежения практически за каждым гражданином.

Можно предположить, что, регулярно узнавая об утечке данных и тотальной правительственной слежке, мы были бы в невероятной ярости. Можно предположить, что, зная, как быстро это произошло — всего за каких-то пару лет, — мы бы испытали шок и вышли бы на улицы с

транспарантами. В действительности же происходит абсолютно противоположное. Многие из нас — даже многие из тех, кто читает эту книгу — в какой-то степени смирились с тем, что все наши действия — телефонные разговоры, текстовые сообщения, электронные письма и страницы в социальных сетях — могут просматриваться и прослушиваться третьими лицами.

И это обескураживает.

Многие из нас — даже многие из тех, кто читает эту книгу — в какой-то степени смирились с тем, что все наши действия — телефонные разговоры, текстовые сообщения, электронные письма и страницы в социальных сетях — могут просматриваться и прослушиваться третьими лицами.

И это обескураживает.

Допустим, вы не нарушаете законов, ведете, по вашему мнению, спокойную и размеренную жизнь и вам кажется, что вы не выделяетесь из толпы других людей в Интернете. Поверьте мне, даже вы не невидимка. По крайней мере, пока.

Я люблю фокусы, а некоторые утверждают, что «ловкость рук» — это необходимое условие для хакерства. Один из известных фокусов заключается в том, чтобы сделать объект невидимым. Однако секрет тут в том, что объект в действительности не исчезает и не становится на самом деле невидимым. Объект всегда остается на месте: на заднем плане, за занавесом, в рукаве, в кармане, там, где мы можем его увидеть… Или не можем.

Это же касается и того множества персональной информации о каждом из нас, которое фиксируется и хранится, часто даже без нашего ведома. Большинство из нас просто не догадывается, насколько легко другой человек может просмотреть эту информацию, и даже не знает, где искать. А раз мы не видим эти данные, то, вероятно, верим, что являемся невидимыми для наших бывших, родителей, учителей, начальников и даже правительства.

Проблема заключается в том, что, если знать, где искать, эта информация доступна абсолютно каждому.

Когда я выступаю перед большим количеством слушателей — размер помещения при этом не имеет значения, — обычно находится кто-то, кто ставит этот факт под сомнение. После одного из таких событий на меня насела очень скептически настроенная журналистка.

Я хорошо помню, как мы сидели за отдельным столиком в баре отеля в одном из американских мегаполисов и журналистка сказала, что она бы никогда не стала жертвой утечки данных. По ее словам, в силу своего юного возраста она была зарегистрирована лишь на очень ограниченном количестве ресурсов и поэтому мало где оставляла свои данные. Она никогда не указывала личную информацию ни в своих статьях, ни в социальных сетях — она старалась не выходить за границы профессионального общения. Она считала себя невидимой. Поэтому я попросил ее разрешения найти в Интернете ее номер социального обеспечения и другие персональные данные. Она согласилась, хоть и неохотно.

Сидя рядом с ней, я вошел в свою учетную запись на сайте, предназначенном для частных детективов. Я, пускай с некоторой натяжкой, подхожу под последнее определение благодаря своей работе, связанной с расследованием хакерских атак по всему миру. Мне уже было известно ее имя, поэтому я спросил, где она живет.

Я также мог бы найти эти сведения в Интернете, на другом сайте, если бы она не сказала мне сама.

Через пару минут я уже знал ее номер социального страхования, город рождения и даже девичью фамилию ее матери. Также я знал все места, где она когда-либо проживала, и все номера телефонов, которые она когда-либо использовала. Уставившись в экран с удивленным выражением лица, она подтвердила, что вся эта информация в той или иной степени верна.

Доступ к этому сайту открыт ограниченному кругу проверенных компаний и специалистов. С пользователей взимают небольшую ежемесячную плату, плюс дополнительно оплачивается каждый информационный запрос, а также время от времени проводят проверки, цель которых — выяснить, по-прежнему ли у меня есть законные основания пользоваться подобным ресурсом.

Но подобного рода информацию об абсолютно любом человеке можно найти за небольшую, однократную плату. И это совершенно законно.

Вы когда-нибудь заполняли форму в Интернете, предоставляли свои данные учебному заведению или организации, которая выкладывает информацию в Интернет, или участвовали в судебном процессе, информация о котором была опубликована в Интернете? Если да, то вы добровольно передали персональную информацию третьему лицу, которое может поступать с ней, как ему заблагорассудится. Существует вероятность, что часть этой информации — если не вся — теперь в Интернете и любая компания, зарабатывающая на сборе персональных данных людей, может ее

получить. Некоммерческая организация «Центр обмена информацией о праве на приватность» (Privacy Rights Clearinghouse) опубликовала сведения более чем о 130 компаниях, которые собирают персональные данные (достоверные и недостоверные) о вас.

А также существуют данные, которые вы не выкладывали в Интернет, но они все равно стали достоянием крупных компаний и правительства, — информация о том, кому мы отправляем электронные письма, текстовые сообщения, кому звоним, что мы ищем в Интернете, что мы покупаем в реальных или интернет-магазинах, ходим ли мы пешком или ездим на машине. Объем данных о каждом из нас с каждым днем растет в геометрической прогрессии.

Возможно, вам кажется, что об этом не стоит беспокоиться. Поверьте мне, стоит. Надеюсь, что, прочитав эту книгу до конца, вы будете достаточно обеспокоены, готовы что-то предпринять и вооружены знанием, что именно нужно делать.

Факты таковы: мы живем с иллюзией, что наша частная жизнь конфиденциальна, и, вероятно, эта ситуации длится уже несколько десятилетий.

Факты таковы: мы живем с иллюзией, что наша частная жизнь конфиденциальна, и, вероятно, эта ситуации длится уже несколько десятилетий.

В определенный момент нас может начать беспокоить то, что правительство, работодатели, начальники, учителя и родители имеют слишком большой доступ к нашей личной жизни. Но поскольку границы этого доступа расширялись постепенно, поскольку мы принимали каждую цифровую технологию, которая делала нашу жизнь чуточку удобнее, не задумываясь о том, как это отразится на нашей приватности, теперь повернуть все вспять становится все труднее и труднее. Кроме того, кто из нас готов отказаться от своих игрушек?

Жить в условиях тотального цифрового контроля со стороны государства опасно не столько тем, что кто-то занимается сбором наших данных (с этим ничего не поделаешь), сколько тем, *как* используются собранные данные.

Представьте себе, что дотошный полицейский или прокурор может сделать с собранным на вас обширным досье непроверенных данных, возможно, за последние несколько лет. Та информация, которая попала в ваше досье сейчас, часто вырванная из контекста, будет храниться вечно. Даже судья Верховного суда Стивен Брайер согласен с тем, что «любому человеку сложно заранее определить, в какой момент имеющиеся документы или факты его биографии могут показаться (обвинителю) важными в том или ином расследовании». Другими словами, выложенная кем-то в социальной сети Facebook ваша фотография в пьяном виде может оказаться наименьшей из ваших проблем.

Возможно, вам кажется, что вам нечего скрывать, но как вы можете быть в этом уверены? Интернет-издание Wired опубликовало хорошо аргументированную статью уважаемого эксперта по безопасности Мокси Марлинспайка, который говорит о том, что в США федеральным преступлением может оказаться нечто, казалось бы, столь незначительное, как, например, держать дома маленького омара. «Не важно, купили ли вы его в продуктовом магазине или кто-то его вам подарил, жив он или мертв, нашли ли вы его уже после того, как он умер собственной смертью, или же убили его в результате самозащиты. Вас могут посадить в тюрьму только за то, что это омар». Суть в том, что в США существует множество незначительных законов, за соблюдением которых никто никогда не следил, а вы, возможно, нарушаете их и даже не подозреваете об этом. Но теперь при этом существует след из данных, служащих уликой против вас, и всего в нескольких кликах от любого, кому они могут понадобиться.

Неприкосновенность личной жизни — это сложный вопрос. Тут нет универсальных советов. У каждого свои причины свободно делиться с незнакомцами определенной информацией о себе и хранить в секрете остальные стороны своей жизни. Возможно, вы просто не хотите, чтобы ваша вторая половина прочитала что-то сугубо личное о вас. Возможно, вы не хотите, чтобы ваш работодатель был в курсе вашей частной жизни. Или возможно, вы всерьез опасаетесь, что за вами следят спецслужбы.

У всех все по-разному, поэтому ни один из советов в этой книге не будет универсальным. Поскольку у всех из нас очень сложное и поэтому очень индивидуальное отношение к вопросу неприкосновенности личной жизни, я расскажу вам о самом важном — о том, что происходит сегодня в сфере тайного сбора данных, — и вы сможете сами решить, что из этого может относиться лично к вам.

В любом случае эта книга поможет вам понять, как обезопасить свою личную информацию в цифровом мире, и предложит варианты решения этой проблемы, которые вы можете взять на вооружение или проигнорировать. Поскольку конфиденциальность — это личное дело каждого, степень «невидимости» также сугубо индивидуальна.

В этой книге я буду говорить о том, что абсолютно за каждым из нас ведется наблюдение — и дома, и вне его стен, когда вы идете по улице, сидите в кафе или едете по шоссе. Компьютер, телефон, машина, домашняя сигнализация и даже холодильник — все это потенциальные точки доступа к вашей частной жизни.

Хорошая новость заключается в том, что я не только буду пугать вас, но и покажу, что делать в условиях отсутствия конфиденциальности — в ситуации, которая стала нормой жизни.

Из этой книги вы узнаете, как:

— Шифровать и отправлять защищенные электронные письма;

— Надежно защищать свои данные с помощью паролей;

— Скрывать свой реальный IP-адрес от сайтов и сервисов, которые посещаете;

— Оберегать компьютер от слежки;

— Сохранять свою анонимность;

— и многое другое.

Теперь приготовьтесь освоить искусство быть невидимым.

Глава 1

ВАШ ПАРОЛЬ МОЖНО ВЗЛОМАТЬ!

У актрисы Дженнифер Лоуренс праздничный уикенд Дня труда выдался напряженным. Лауреат премии «Оскар» оказалась среди тех знаменитостей, которые в 2014 году одним прекрасным утром узнали, что их интимные снимки — на многих она была изображена в обнаженном виде — были выложены в Интернет.

Остановитесь и прокрутите в голове все фотографии, которые в данный момент хранятся на вашем компьютере, смартфоне и в электронном ящике. Скорее всего, большинство из них абсолютно безобидные. Вас бы вряд ли сильно огорчило, если бы весь мир увидел закаты, милые семейные снимки и даже, может быть, дурацкие шутливые селфи. Но хотелось бы вам, чтобы люди увидели абсолютно каждую фотографию? Что бы вы почувствовали, если все бы они вдруг попали в Интернет? Да, не все наши личные снимки непристойны, но все же это наша частная жизнь. Мы должны иметь право самостоятельно решать, как, где и когда ими делиться и делиться ли ими вообще. Но облачные сервисы часто лишают нас такой возможности.

Произошедшая с Дженнифер Лоуренс история обсуждалась во всех новостях в тот выходной в честь Дня труда 2014 года. В СМИ это событие окрестили как «Fappening» (от англ. *happening* (событие) + *fap* (мастурбировать)): в Интернет попали фотографии Рианы, Кейт Аптон, Кейли Куоко, Эдрианн Карри и почти трехсот других звезд, в основном женщин, к чьим снимкам со смартфонов каким-то образом получили доступ злоумышленники. Хотя некоторые, как и следовало ожидать, с радостью воспользовались ситуацией, для других этот случай стал тревожным напоминанием о том, что такое может произойти и с ними.

Так как же кто-то получил доступ к личным фотографиям Дженнифер Лоуренс и других знаменитостей?

Поскольку у всех звезд был iPhone, тут же начались разговоры о масштабной утечке данных из созданного компанией Apple сервиса iCloud, облачного хранилища данных для владельцев iPhone. Когда на самом устройстве заканчивается память, ваши фотографии, новые файлы, музыка и игры сохраняются на сервере Apple, обычно за небольшую ежемесячную плату. Google предоставляет аналогичный сервис пользователям Android.

Компания Apple, которая практически никогда не комментирует сообщения в СМИ, касающиеся вопросов информационной безопасности, отрицала возможность какой-либо утечки со своей стороны. Компания, вопреки обыкновению, опубликовала официальное обращение, в котором назвала инцидент «очень прицельной атакой на имена пользователей, пароли и контрольные вопросы» и добавила, что «результаты расследования ни в одном из рассмотренных случаев не указывают на какую-либо утечку из систем Apple, включая функции iCloud и “Найти iPhone”».

Как же вышло, что посторонние получили удаленный доступ к частным материалам?

Фотографии сначала появлялись на хакерском форуме, который известен тем, что на нем часто выкладывают краденые фотографии. На этом форуме активно обсуждаются инструменты криминалистической экспертизы цифровых средств, с помощью которых можно было бы тайно получить подобные фотографии. С помощью таких инструментов технические специалисты, детективы и сотрудники правоохранительных органов извлекают данные с устройства или из «облака» в ходе расследования преступления. И конечно, такими инструментами пользуются также совсем другие люди.

Один из инструментов, открыто обсуждавшихся на форуме, называется Elcomsoft Phone Password Breaker (EPPB). Он разработан для того, чтобы правоохранительные органы и спецслужбы могли получать доступ к учетным записям пользователей iCloud, и его может купить каждый желающий. Это лишь одно из обсуждавшихся на форуме средств, но, по всей видимости, наиболее популярное там. Для работы с EPPB необходимо сначала выяснить логин и пароль от нужной учетной записи в iCloud. Однако для общающихся на этом форуме получить подобные сведения, видимо, не проблема. По стечению обстоятельств в тот же самый праздничный день в 2014 году кто-то выложил на популярный сервис-репозиторий для хранения программного кода (GitHub) механизм для взлома паролей под названием iBrute, созданный специально для сбора авторизационных данных любых учетных записей iCloud.

Применив обе программы (iBrute и EPPB) одновременно, можно получить данные для входа в учетную запись iCloud и скачать на свое устройство все резерные копии информации с iPhone жертвы, которые хранятся в «облаке». Это очень удобная опция, если вы, к примеру, обновляете операционную систему своего смартфона. Также это бесценный источник сведений для хакера, который теперь видит все, что вы когда-либо делали на смартфоне. Он получает гораздо больше сведений, чем если бы просто вошел в чью-то учетную запись iCloud.

Джонатан Здзиарски, консультант по восстановлению паролей и данных в интересах правоохранительных органов и специалист по информационной безопасности, рассказал интернет-изданию Wired, что, изучив вопрос утечки фотографий, он пришел к выводу, что, например, в случае с Кейт Аптон, вполне могли применяться инструменты iBrute и EPPB. Доступ к хранилищу резервных копий со смартфона iPhone открывает хакеру более личную информацию, которую позже можно использовать для шантажа.

Осенью 2014 года агенты ФБР пришли в частный дом в южной части Чикаго, который Apple смогла по IP-адресу связать с несанкционированным доступом более чем к 500 аккаунтам iCloud, причем более чем к 300 из них доступ осуществлялся несколько раз. На момент передачи этой книги в печать никаких обвинений предъявлено не было.

Что здесь интересно, Elcomsoft продает свои программные продукты и правоохранительным органам, и обычной публике. Знать, что полиция может провести на сайт, защищенный паролями, атаку методом грубой силы, это одно. Знать, что это может сделать безвестный житель Чикаго — совсем другое. В этой главе мы поговорим о том, как защитить ваши онлайн-аккаунты и устройства при помощи паролей.

В результате расследования правоохранительные органы вышли на 36-летнего жителя Ланкастера, штат Пенсильвания, Райана Коллинза, которого в октябре 2016 года приговорили к 18 месяцам тюрьмы за «незаконный доступ к защищенному компьютеру с целью получения информации». Его обвинили в незаконном доступе к ста с лишним аккаунтам Apple и почтовым ящикам Google.

Чтобы защитить свою учетную запись в iCloud и других сервисах, необходимо придумать надежный пароль. Это очевидно. И все же, как человек, который занимается проверкой систем на уязвимость (т. е. человек, которому платят за взлом компьютерных сетей, чтобы найти слабые места), я знаю, что многим людям — даже топ-менеджерам крупных корпораций — обычно лень придумывать хороший пароль. Задумайтесь над тем, что у генерального директора компании Sony Entertainment Майкла Линтона основным паролем был «sonyml3». Неудивительно, что его почту взломали и выложили письма в Интернет, ведь у хакеров были административные права доступа практически ко всем системам компании.

Помимо рабочих паролей существуют пароли, которые защищают персональные данные. Даже трудный пароль хакерские инструменты, такие как oclHashCat (инструмент подбора пароля, задействующий ресурсы видеокарты), могут взломать, но процесс перебора будет настолько длительным, что злоумышленник скорее решит переключиться на другую, более легкую мишень.

Вполне можно допустить, что некоторые из паролей, обнародованных после взлома сайта Ashley Madison в июле 2015 года, используются и в другом контексте — в том числе для доступа к банковским счетам и даже к рабочим компьютерам. В выложенном в Интернет списке из 3,3 миллиона паролей к сайту Ashley Madison самыми распространенными оказались «123456», «12345», «password», «DEFAULT», «123456789», «qwerty», «12345678», «abc123» и «1234567». Если среди перечисленного вы увидели свой пароль, ваши данные вполне могут быть похищены, поскольку эти варианты паролей включены в большинство доступных в Интернете инструментов для подбора паролей. Чтобы проверить, не было ли утечки регистрационных данных какой-либо из ваших учетных записей, зайдите на сайт .

В двадцать первом веке мы способны на большее. На гораздо большее. Мы можем придумывать значительно более длинные и сложные сочетания букв и цифр. Может показаться, что здесь могут возникнуть какие-либо трудности, но я продемонстрирую вам два способа справиться с данной задачей: вручную и автоматически.

Самая простая тактика — вместо того чтобы придумывать пароли самостоятельно, автоматизируйте этот процесс. В Интернете можно найти множество менеджеров паролей. Они хранят пароли в защищенном электронном хранилище и предоставляют вам быстрый доступ к ним, когда необходимо, также, если требуется, они генерируют новые, надежные, уникальные пароли для каждого сайта.

Однако с этой тактикой связаны две проблемы. Во-первых, для доступа к менеджеру паролей нужен главный пароль (называемый мастер-паролем). Если кто-нибудь сумеет установить на ваш компьютер вредоносную программу-кейлоггер (клавиатурный шпион), которая украдет вашу базу данных с паролями и тот самый главный пароль, пиши пропало. Тогда у хакера будет доступ ко всем вашим паролям. Проверяя системы на уязвимость, мы иногда заменяем менеджер паролей на версию с подвохом, которая пересылает пароль нам (конечно, при условии, что установлен менеджер паролей с открытым исходным кодом). Это делается после того, как мы получаем административные права доступа к клиентской сети. Затем мы узнаем пароли. Другими словами, менеджер паролей служит нам черным ходом, войдя через который мы получаем ключи от королевства.

Вторая проблема достаточно очевидна: если вы утратите главный пароль, вы утратите все свои

пароли (что не так страшно, на каждом отдельном сайте всегда можно восстановить пароль, о чем мы поговорим через минуту, но если у вас много разных учетных записей, это доставит массу хлопот).

Несмотря ни на что, следующие советы вполне способны помочь вам защитить свой пароль.

Во-первых, надежный пароль — это длинный пароль, не менее 20–25 символов. Лучший вариант — случайные наборы символов, например ek5iogh#skf&skd. К сожалению, человеческий мозг с трудом запоминает случайные последовательности. Поэтому пользуйтесь менеджером паролей. Это гораздо лучше, чем придумывать пароль самостоятельно. Я предпочитаю менеджеры паролей с открытым кодом, такие как Password Safe и KeePass, они хранят данные только на вашем компьютере.

Важное правило — никогда не устанавливайте один и тот же пароль на два разных аккаунта. Сложно следовать этому правилу. В наше время пароль необходимо придумывать практически для всего на свете. Поэтому обзаведитесь менеджером паролей, который будет создавать и хранить надежные, уникальные пароли.

К счастью, большинству из нас противостоит не государство, располагающее практически безграничными ресурсами и временем. Чаще всего нами интересуются супруги, родственники или кто-то, кому мы насолили, т. е. люди, которые, столкнувшись с паролем длиной в 25 символов, не смогут его взломать, поскольку не располагают необходимым временем и ресурсами.

Даже если пароль надежен, его можно обойти с помощью ряда технологий. Существуют программы угадывания паролей, например John the Ripper, бесплатная программа с открытым кодом, которую может скачать кто угодно. Пользователь настраивает фильтры и запускает программу. В частности, можно указать количество символов, наличие или отсутствие специальных символов, добавить иноязычную раскладку и прочее. Утилита John the Ripper и другие программы для перебора паролей способны переставлять буквы пароля по определенным правилам, повышающим эффективность работы. Это означает всего лишь то, что программа просто проверяет каждую возможную комбинацию чисел, букв и символов, подходящую под заданные параметры, до тех пор, пока не подберет нужный пароль. К счастью, большинству из нас противостоит не государство, располагающее практически безграничными ресурсами и временем. Чаще всего нами интересуются супруги, родственники или кто-то, кому мы насолили, т. е. люди, которые, столкнувшись с паролем длиной в 25 символов, не смогут его взломать, поскольку не располагают необходимым временем и ресурсами.

Допустим, вы решили создать пароли по старинке и подобрали максимально сложные комбинации. Угадайте, что дальше? Можно записать их. Просто не пишите что-нибудь в духе «Сбербанк: тыне1окпосмо3насвет*». Это слишком очевидно. Лучше вместо названия банка (например) напишите что-нибудь зашифрованное, скажем «банка с печеньем» (потому что некоторые люди прячут сбережения в банках из-под печенья), и далее «тыне1ок». Обратите внимание, я не закончил парольную фразу. И вам не нужно. Вы знаете, что там дальше. Но кто-то другой не знает.

Любой, обнаруживший листок с незаконченными паролями, будет изрядно сбит с толку — по крайней мере, в первый миг. Любопытный случай: я был в гостях у друга — очень известного сотрудника корпорации Microsoft, — и за ужином мы с его женой и детьми говорили о надежности паролей. В какой-то момент жена друга встала и подошла к холодильнику. Она записала все свои пароли на листе бумаге и прикрепила его к дверце с помощью магнитика. Друг только покачал головой, а я расплылся в широкой улыбке. Записывать пароли, возможно, не лучшее решение, но ничуть не лучше забыть редко используемый сложный пароль.

Некоторые сайты — например, интернет-банк — блокируют пользователей после нескольких неудачных попыток ввести пароль: как правило, речь идет о трех попытках. Однако многие сайты этого не делают. Но даже если сайт приостанавливает пользователю доступ после трех неудачных попыток, это не спасает от злоумышленников с программами вроде John the Ripper или oclHashcat. (oclHashcat задействует несколько графических процессоров и потому гораздо мощнее, чем John the Ripper). Кроме того, хакеры не проверяют каждый возможный вариант пароля на реальном сайте.

Представим себе, что произошла утечка и среди скомпрометированных данных оказываются логины и пароли. Но в паролях, полученных таким образом, творится настоящий хаос.

Как с помощью всего этого кто-либо сможет попасть в вашу учетную запись?

Каждый раз при вводе пароля, будь то для разблокировки ноутбука или для входа в учетную запись в вебсервисе, к этому паролю применяется однонаправленный алгоритм, известный как хеш-функция. Это не то же, что шифрование. Шифрование представляет собой двусторонний процесс: то, что зашифровано, можно расшифровать, если у вас есть ключ. Хеш-функция — это однозначное преобразование исходных данных в последовательность символов. Теоретически однонаправленная функция необратима — по крайней мере, восстановить исходные данные не так просто.

В базе данных с паролями, хранящейся на обычном компьютере, смартфоне или в «облаке», информация представлена не как «УМэриБылБарашек123$», а в хешированном виде, т. е. как зашифрованная последовательность цифр и букв. Эта последовательность и представляет ваш пароль.

Таким образом, именно хеши паролей, а не они сами, хранятся в защищенной области памяти компьютера и именно их получают хакеры в результате взлома целевых систем или утечки данных. Получив хеши паролей, хакер может использовать программы наподобие John the Ripper и oclHashcat для их расшифровки либо методом перебора (проверки каждой возможной комбинации букв и цифр), либо пробуя каждое из слов списка, например словаря. Настройки в программах John the Ripper и oclHashcat позволяют хакерам при подборе паролей преобразовывать слова по различным шаблонам, например по шаблону, который называется leetspeak (или просто leet) и представляет собой систему замены латинских букв цифрами, как в «k3vln ml7nlck». Благодаря этому шаблону все пароли можно заменить на различные модификации на языке leetspeak. Эти методы позволяют с гораздо большей эффективностью взламывать пароли, чем при простом методе перебора (или брутфорсе, «метод грубой силы», как его еще называют). Самые простые и распространенные пароли без труда взламываются в первую очередь, а на взлом более сложных паролей требуется больше времени. Объем этого времени зависит от ряда факторов. С помощью инструмента для взлома паролей и ваших скомпрометированных данных (логин и хеш пароля) злоумышленники получат доступ к одному или нескольким вашим аккаунтам, применив этот же пароль к другим сервисам, подключенным к вашей электронной почте или иному идентификатору.

В целом, чем больше в пароле символов, тем больше времени потребуется таким программам, как John the Ripper, чтобы испробовать все возможные варианты. Однако чем мощнее становятся процессоры, тем меньше времени требуется на вычисление всех возможных паролей, состоящих из шести и даже из восьми символов. Именно поэтому я рекомендую использовать пароли не короче 25 символов.

После того как вы придумали надежный пароль, даже несколько надежных паролей, никогда никому их не сообщайте. Кажется, что это совершенно очевидно, но несколько опросов общественного мнения в Лондоне и других крупных городах показали, что люди готовы раскрыть свои пароли в обмен на нечто совершено незначительное, например, на ручку или шоколадку.

Мой друг как-то поделился паролем к сервису Netflix со своей девушкой. Казалось, что это логичный поступок. Смысл был в том, чтобы она выбрала фильм для совместного просмотра. Но ловушка скрывалась в разделе с рекомендациями Netflix — они составляются на основе ранее просмотренных фильмов, часть из которых мой друг смотрел вместе с предыдущими девушками. Например, очевидно, что комедию «Джинсы-талисман» он не стал бы заказывать для себя самого, и его девушка это понимала.

Конечно, у всех есть бывшие. Если ваш партнер утверждает, что у него (или нее) раньше никого не было, это, скорее, странно. Но ни одна девушка не пожелает столкнуться лицом к лицу с напоминанием о своих предшественницах.

Если доступ к вашим онлайн-аккаунтам защищен паролем, необходимо также устанавливать пароль и на персональные устройства. У большинства из нас есть ноутбуки, а у многих до сих пор есть настольные компьютеры. Возможно, вы целый день проводите дома в одиночестве. Но что, если вы пригласите на ужин гостей? Вдруг кто-нибудь из них откроет ваши файлы, фотографии или игры, просто сев за ваш стол и передвинув мышку? Еще одна поучительная история, связанная с Netflix: когда-то давно, когда этот сервис занимался рассылкой DVD, я был знаком с парой, которая стала жертвой розыгрыша. Они устроили дома вечеринку и не закрыли на компьютере вкладку с личным кабинетом на сайте Netflix в браузере. Впоследствии эта пара оказалась подписана на порнографические фильмы всех сортов (они обнаружили это, только когда получили по почте второй или третий DVD).

Еще важнее защищать себя паролями в офисе. Только подумайте о том, сколько раз вам приходилось покидать свое рабочее место ради спонтанного совещания. Кто угодно мог, проходя мимо вашего стола, увидеть таблицу с бюджетом на следующий квартал. Или все электронные письма в вашем ящике. Хуже того, если вы отойдете от рабочего стола надолго (например, на обед или длительное собрание) и у вас не установлена экранная заставка, включающаяся через пару секунд отсутствия активности, кто-то может сесть, написать электронное письмо и отправить его от вашего имени. Или даже изменить проект бюджета на следующий квартал.

Существуют новые хитроумные способы избежать подобного поворота событий, например программа блокировки экрана, которая определяет, насколько вы далеко от компьютера, с помощью технологии Bluetooth. Иными словами, если вы вышли в туалет и ваш смартфон оказался вне радиуса действия Bluetooth, экран тут же заблокируется. Также существуют программы, ориентирующиеся на Bluetooth-сигналы таких устройств, как умные часы или браслеты.

Создание паролей для защиты учетных записей в Интернете — это одно, но это не поможет вам,

если кто-то физически завладеет устройством, особенно если вы не вышли из этих учетных записей. Если бы можно было установить пароль только на какой-то один тип устройств, то остановить выбор необходимо было бы на мобильных устройствах, поскольку они наиболее подвержены утрате или хищению. И все же, согласно данным издания Consumer Reports, 34 процента американцев совсем не защищают мобильные устройства, даже простейшим 4-символьным пин-кодом.

В 2014 году в полицейском участке города Мартинес, штат Калифорния, произошел следующий инцидент.

Оказалось, что сотрудник полиции украл интимные фотографии со смартфона женщины, задержанной за вождение в нетрезвом виде, что представляет собой явное нарушение четвертой поправки к конституции США, входящей в состав Билля о правах. В частности, четвертая поправка запрещает производить необоснованные обыски и изъятие имущества без выданного судьей ордера и без веского довода — сотрудники правоохранительных органов должны объяснить, зачем им необходимо проверить содержимое телефона.

Если вы до сих пор не установили пароль на смартфон, сделайте это сейчас, потратьте минуту своего времени. Я серьезно.

Существует три основных типа блокировки экрана смартфона — будь то устройство под управлением Android, iOS или какой-либо другой операционной системы. Самый распространенный — это код доступа, последовательность цифр, которые необходимо ввести в определенном порядке, чтобы разблокировать смартфон. Не назначайте код, состоящий из рекомендованного по умолчанию количества цифр. Перейдите в раздел настроек и вручную установите длину пароля в 7 цифр или более (указав, например, ваш старый номер телефона). Во всяком случае, длина пароля должна быть точно больше 4 цифр.

На некоторые мобильные устройства можно устанавливать пароль, содержащий буквы, как, например, тот, о котором мы говорили выше. Опять же предпочтительная длина составляет 7 символов. Современные мобильные устройства отображают одновременно как буквенные, так и цифровые символы, благодаря чему стало гораздо проще чередовать буквы с цифрами.

Третий вариант блокировки — графический ключ. Начиная с 2008 года, на смартфонах под управлением операционной системы Android присутствует функция под названием Android Lock Patterns (ALP). На экране отображаются девять точек, вы соединяете их в любом порядке, и эта последовательность соединения становится вашим паролем. Возможно, вы думаете, что это гениальное изобретение и что обширный диапазон возможных комбинаций делает ваш ключ неуязвимым. Но человеческую натуру не изменить, и на конференции PasswordsCon в 2015 году ученые заявили, что хотя существует более 140 704 вариаций графических ключей, участники исследования предпочитали использовать всего несколько из них. Какие же графические ключи оказались самыми распространенными? Часто это первая буква имени человека. Исследование также показало, что люди предпочитают задействовать центральные точки и редко включают в комбинацию угловые точки. Примите это во внимание, когда будете придумывать себе следующий графический ключ.

Помимо прочего, существует биометрическая защита. Компании Apple, Samsung и другие популярные производители в настоящее время позволяют пользователям для разблокировки телефонов использовать сканер отпечатков пальцев. Следует знать, что они не обеспечивают стопроцентной защиты. После появления технологии TouchID исследователи — по крайней мере, те, которые ожидали, что компания Apple усовершенствует существовавшие и прежде сканеры отпечатков пальцев — с удивлением обнаружили, что несколько старых способов обхода блокировки срабатывают и на iPhone.

Например, можно снять отпечаток пальца с чистой поверхности, используя детскую присыпку и липкую ленту.

Некоторые модели смартфонов оснащены функцией распознавания лица владельца. Их также можно обмануть, поднеся к камере фотографию с высоким разрешением.

В целом биометрические данные как таковые уязвимы для хакеров. В идеале биометрия должна быть лишь одним из нескольких этапов идентификации владельца. Оставьте слегка смазанный отмечаток пальца или улыбнитесь в камеру, а затем введите PIN-код или пароль. Так ваше мобильное устройство будет в безопасности.

Что, если вы придумали надежный пароль, но не записали его? Восстановление пароля — это отличный вариант, когда вы никак не можете войти в редко используемую учетную запись. Но это также и легкая мишень для потенциальных взломщиков. С помощью подсказок, которыми изобилуют наши профили в социальных сетях, хакеры могут получить доступ к нашим электронным ящикам — или другим сервисам, — просто сбросив старый пароль.

В СМИ рассказывали о мошеннике, который узнал четыре последние цифры номера банковской карты своей жертвы, а затем использовал эту информацию как средство подтверждения личности во время телефонного разговора со службой поддержки. В поддержку он звонил, чтобы сменить электронный адрес, привязанный к учетной записи в одном из сервисов. Так злоумышленник может сменить пароль на свой собственный, а владелец аккаунта даже не будет об этом знать.

В 2008 году студент университета Теннесси Дэвид Кернелл решил посмотреть, получится ли у него взломать на сайте Yahoo! личный электронный ящик Сары Пэйлин, кандидата на пост вице-президента. Кернелл мог бы попробовать подобрать пароль, но доступ к ящику был бы заблокирован после нескольких неудачных попыток. Вместо этого он воспользовался функцией сброса пароля — позже он описал этот процесс как «простой».

Я уверен, что такое случалось с каждым из нас: сначала вы получаете странное письмо от друга и знакомого со ссылкой на иностранный порносайт, а потом выясняется, что его электронный ящик был взломан. Часто это происходит из-за слабого пароля. Или же кто-то просто узнал пароль — в результате утечки или использования функции сброса пароля.

В момент создания аккаунта — любого, например, почтового или на сайте банка — вам могут задать так называемые секретные вопросы. Обычно их три штуки. Часто сервис предлагает раскрывающийся список с вариантами вопросов, и вы можете выбрать, на какие из них отвечать. Как правило, эти вопросы довольно очевидны.

Где вы родились? В какой школе вы учились? Или институте? И вечный фаворит — девичья фамилия матери, вопрос, который используется в качестве секретного, наверное, минимум с 1882 года. Как вы узнаете чуть позже, компании могут (и с удовольствием это делают) сканировать Интернет в поисках персональных данных, с помощью которых можно без труда ответить на любой распространенный секретный вопрос. Всего пара минут в Интернете — и у вас есть ответы на практически любой секретный вопрос конкретного человека.

Только недавно эти секретные вопросы стали понемногу обновляться. Например, вопрос «В каком городе родился ваш шурин?» довольно редкий (хотя правильно отвечая на такие «хорошие» вопросы, вы также рискуете, о чем я расскажу чуть ниже). Но множество так называемых секретных вопросов по-прежнему очень просты, например: «Кличка вашего домашнего животного?»

В целом, устанавливая секретные вопросы, постарайтесь избегать наиболее очевидных вариантов из раскрывающегося списка. Даже если сайт предлагает только распространенные вопросы, обратитесь к своему воображению. Кто сказал, что ответы обязательно должны быть честными? Проявите смекалку. Например, только для потокового видеосервиса вашим любимым цветом может стать «тутти-фрутти». Кто узнает? Это же цвет, верно? Информация, которую вы указываете в качестве ответа, становится «правильным» ответом на секретный вопрос.

Когда вы придумываете ответы, обязательно записывайте и сам вопрос, и ответ на него и храните эту подсказку в надежном месте (или просто пользуйтесь менеджером паролей). Может так случиться, что когда-нибудь, обратившись в службу технической поддержки, вам нужно будет ответить на один из своих секретных вопросов. Носите с собой в кошельке карточку или блокнотик, который поможет вам вспомнить, что на вопрос: «Где вы родились?», вы ответили: «В роддоме» (или запомните и постоянно используйте один и тот же набор ответов). Эта простая хитрость собьет с толку того, кто собирал о вас информацию в Интернете и попытался дать более правдоподобный ответ, например: «Кировск, Мурманская область».

Отвечая правильно на редкие секретные вопросы, вы еще больше рискуете: вы выдаете личную информацию сверх той, что уже доступна. Например, сайт, на котором вы честно ответили на вопрос: «В каком городе родился ваш шурин?», теперь может продать этот ответ, и вполне возможно, вместе с другими данными. Или же с помощью этого ответа кто-то сможет восполнить пробелы в собранных сведениях. Например, по ответу на этот вопрос можно узнать, что вы женаты (или были женаты), что у вашей жены (или бывшей жены) есть брат, родившийся в указанном городе. Для одного простого ответа это очень много дополнительной персональной информации. С другой стороны, если у вас нет шурина, вперед — отвечайте с фантазией, например: «Пуэрто-Рико». Это собьет с толку любого, кто собирает на вас досье. Чем больше ложных данных вы предоставите, тем лучше защитите свою конфиденциальность в Интернете.

Отвечая на менее распространенные секретные вопросы, всегда взвешивайте, насколько тот или иной сайт ценен для вас (например, можно доверить дополнительные персональные сведения своему банку, но никак не потоковому видеосервису). Также обращайте внимание на политику конфиденциальности (ищите формулировки, которые прямо свидетельствуют или косвенно намекают на то, что сайт может продавать собранные данные третьим лицам).

Для сброса пароля электронной почты Сары Пэйлин потребовалась ее дата рождения, почтовый индекс и ответ на секретный вопрос: «Где вы познакомились с мужем?» Дату рождения и почтовый

индекс Пэйлин без труда можно было найти в Интернете (в тот момент Пэйлин была губернатором штата Аляска). Чтобы ответить на секретный вопрос, пришлось приложить чуть больше усилий, но Кернелл сумел найти нужную информацию. Пэйлин давала множество интервью и из раза в раз повторяла, что в своего мужа она влюблена еще со старших классов школы. Таким образом, ответ на секретный вопрос: «Старшие классы школы».

Отгадав ответ на секретный вопрос Пэйлин, Кернелл смог сбросить пароль от ее ящика Yahoo! и сменить его на новый. Так ему удалось прочитать всю личную переписку политика. Снимок экрана с ее папкой «Входящие» был выложен на хакерском ресурсе. Сама же Пэйлин не могла войти в свою почту, пока не сбросила пароль.

Поступок Кернелла был противозаконным, он нарушил закон «О компьютерном мошенничестве и злоупотреблении с использованием компьютеров». Его признали виновным по двум пунктам обвинения: препятствование правосудию путем уничтожения улик и незаконный доступ в компьютерную систему. В 2010 году его приговорили к тюремному заключению сроком один год и один день плюс три года профилактического наблюдения после освобождения.

Если вашу почту взломали так же, как почту Пэйлин, в первую очередь необходимо сменить пароль, сбросив его (вы, наверное, уже догадались сами). Пусть новый пароль будет надежнее, как мы только что говорили. Далее проверьте папку с отправленными от вашего имени письмами. Возможно, вы найдете там письмо со спамом со множеством адресатов из вашего списка контактов. (Теперь-то вы понимаете, почему все эти годы ваши друзья шлют вам спам — кто-то взламывает их электронную почту.)

Также проверьте, вдруг кто-то связал свой аккаунт с вашим. Хакер, получивший доступ к вашему ящику, также может настроить переадресацию ваших писем на свою почту. Вы, как и прежде, будете пользоваться почтовым ящиком в обычном режиме, но другой человек тоже будет читать ваши письма. Если кто-то связал свой аккаунт с вашим, немедленно удалите ящик для переадресации.

Пароли и коды безопасности частично решают проблему безопасности, но мы только что видели, что их можно подобрать. Гораздо эффективнее сложных паролей вас защитит двухфакторная аутентификация.

Пароли и коды безопасности частично решают проблему безопасности, но мы только что видели, что их можно подобрать. Гораздо эффективнее сложных паролей вас защитит двухфакторная аутентификация. После скандала с утечкой фотографий обнаженной Дженнифер Лоуренс и других знаменитостей компания Apple разработала новый метод контроля доступа к сервисам iCloud — двухфакторную аутентификацию.

Что такое двухфакторная аутентификация?

При аутентификации пользователя на сайтах и сервисах необходимо подтверждение как минимум двух пунктов из трех. Обычно это: что-то, что у вас есть, что-то, что вы знаете, и что-то, чем вы являетесь. Этим чем-то может быть банковская карта с магнитной полосой или чипом. Чем-то, что вы знаете, чаще всего бывает PIN-код или ответ на секретный вопрос. А что-то, чем вы являетесь, включает в себя биометрические данные — сканер отпечатков пальцев, распознавание лиц, распознавание голоса и пр. Чем больше данных совпадает, тем выше вероятность того, что пользователь является именно тем, за кого себя выдает.

Ничего нового в этом нет. Уже более сорока лет большинство из нас пользуются двухфакторной аутентификацией, сами того не осознавая.

Каждый раз, снимая деньги в банкомате, вы проходите через двухфакторную аутентификацию. Как это? У вас есть выпущенная банком карта, вы знаете PIN-код. Сочетание этих двух факторов говорит уличному банкомату, что вы хотите получить доступ к счету, к которому привязана карта. В некоторых странах в банкоматах присутствуют дополнительные средства проверки, например, распознавание лиц и сканер отпечатка ладони. Это уже многофакторная аутентификация.

Нечто подобное возможно и в Интернете. Различные финансовые и медицинские организации, а также коммерческие сервисы электронной почты и социальные сети позволяют настраивать двухфакторную аутентификацию. В этом случае тем, что вы знаете, будет пароль, а тем, что у вас есть, — сотовый телефон. При получении доступа к этим сайтам телефон — это «внешний фактор», поскольку он никак не связан с используемым компьютером. Однако при настроенной двухфакторной аутентификации хакер не сможет получить доступ к вашей учетной записи, если у него не будет вашего телефона.

Допустим, у вас есть учетная запись на сервисе Google Gmail. Чтобы подключить двухфакторую аутентификацию, вам нужно будет ввести номер сотового телефона. Для проверки вашей личности Google отправит вам SMS-сообщение с шестизначным кодом. Вы будете должны ввести этот код на

сайте Gmail, подтвердив тем самым, что данный компьютер связан с данным сотовым телефоном.

После этого, если кто-то с другого компьютера или устройства попытается сменить пароль к вашей учетной записи, вам на телефон придет текстовое сообщение. Любое изменение в настройках учетной записи будет сохранено только после ввода правильного кода подтверждения.

Но и тут есть слабая сторона. Сотрудники компании Symantec выяснили, что при отправке SMS-сообщения для подтверждения личности человек, которому известен ваш номер мобильного телефона, прибегнув к социальной инженерии, может перехватить проверочный код и сбросить пароль, стоит вам лишь утратить бдительность.

Представим, что я хочу взломать вашу почту и не знаю пароль, но знаю номер сотового телефона, поскольку эту информацию легко найти через Google. Я могу перейти на страницу восстановления пароля и запросить сброс пароля. Поскольку у вас настроена двухфакторная аутентификация, вы получите SMS-сообщение с кодом. Пока все в порядке, правда? Не спешите.

Недавно произошел инцидент с политическим активистом Диреем Маккиссоном, телефон которого был взломан. Эта атака стала ярким примером того, как злоумышленники могут обманом получить у оператора сотовой связи сменную SIM-карту. Другими словами, мошенник может завладеть вашим номером телефона и получать приходящие вам SMS-сообщения — например, SMS-код от сервиса Google для сброса пароля от принадлежащего Маккиссону аккаунта Gmail, на котором была настроена двухфакторная аутентификация. Это почти то же самое, что обманом заставить кого-то прочитать вам вслух SMS-сообщение с новым паролем. Хотя и такую возможность (социальную инженерию) никто не отменял.

Поскольку я не вижу код подтверждения, который сервис электронной почты отправил вам по телефону, мне придется притвориться кем-то другим, чтобы вы сами мне его предоставили. Всего за несколько секунд до того, как вы получите настоящее сообщение, например от сервиса Google, я, будучи хакером, могу с одноразового виртуального номера отправить ложное SMS-сообщение со следующим текстом:

«Google обнаружил подозрительную активность в вашем аккаунте. Для прекращения нежелательных действий в аккаунте, пожалуйста, в ответ на это сообщение отправьте проверочный код, высланный на ваше мобильное устройство».

Вы увидите, что да, действительно, вам только что пришло SMS-сообщение от Google с проверочным кодом, и, если вы не очень осторожны, вы можете просто отправить его мне в ответ на фальшивое сообщение. После этого у меня будет не более шестидесяти секунд на то, чтобы ввести код подтверждения на странице сброса пароля. Далее я смогу сменить пароль и захватить вашу почту. Или любую другую почту.

Поскольку SMS-сообщения с кодами не шифруются и код можно узнать тем способом, который я только что описал, для большей надежности рекомендуется скачать приложение для двухфакторной аутентификации Google Authenticator из Google Play или App Store для использования с iPhone. Это приложение генерирует уникальный код доступа, который нужно вводить в самом приложении каждый раз, когда вы хотите посетить сайт с двухфакторной аутентификацией — никаких SMS-сообщений. Шестизначный код, сгенерированный приложением, синхронизируется с механизмом авторизации на сайте, и вы получаете доступ на сайт. Однако приложение Google Authenticator хранит алгоритм генерации одноразовых паролей в системе под названием «Связка ключей iCloud», где задана настройка «Только на этом устройстве». Это означает, что, если вы сделаете резервную копию всех файлов со своего смартфона iPhone, а затем восстановите их на *другом* устройстве (например, купив новый смартфон после потери старого), коды из приложения Google Authenticator на новое устройство перенесены не будут и, чтобы восстановить их, придется изрядно потрудиться. На такой случай лучше заранее распечатать несколько кодов восстановления. Восстановить все свои пароли из резервной копии можно в некоторых других приложениях, например 1Password.

Зарегистрировав устройство в этом приложении, вы будете получать новый код при каждой авторизации в приложении с данного устройства (если не установите флажок доверять этому устройству в течение 30 дней), даже если вы переместите свой ноутбук или телефон в другое место. Однако если вы попытаетесь войти в этот аккаунт с другого устройства — например, с компьютера жены, — тогда потребуется дополнительная аутентификация. Стоит ли говорить, что, если у вас настроена двухфакторная аутентификация, держите сотовый телефон под рукой.

Учитывая все перечисленные выше меры предосторожности, возможно, вы захотите узнать, что я советую людям, осуществляющим любые финансовые операции через Интернет.

Примерно за 2500 рублей в год можно приобрести антивирус и брандмауэр на три компьютера. Проблема заключается в том, что во время путешествия по Всемирной паутине вы можете случайно загрузить в своем браузере рекламный баннер с вредоносным программным обеспечением. Или вы

можете открыть электронную почту, и одно из писем окажется с вирусом. Так или иначе, ваш компьютер будет заражен, если вы регулярно выходите с него в Интернет, и даже антивирус не может уберечь вас от всех опасностей.

Смысл в том, чтобы у вас появилось устройство, которым вы будете пользоваться исключительно для проведения финансовых операций и, может быть, решения медицинских вопросов.

Поэтому я советую вам потратить пару сотен долларов и купить хромбук — ноутбук на базе операционной системы Chrome OS. Мне нравятся планшеты iPad, но они дорогие. Хромбук так же удобен в работе, как и iPad, но гораздо дешевле.

Смысл в том, чтобы у вас появилось устройство, которым вы будете пользоваться исключительно для проведения финансовых операций и, может быть, решения медицинских вопросов. Даже если устройство принадлежит вам, не входите с использованием учетной записи администратора — это даст злоумышленнику возможность устанавливать свое программное обеспечение. Вместо этого используйте учетную запись гостя (Guest), под которой обычно запрещено устанавливать что-либо без разрешения администратора системы. После этого на хромбуке вы сможете устанавливать приложения только из магазина Google Play. Войдя туда, скачайте приложение вашего банка или медицинского учреждения.

Далее настройте двухфакторную аутентификацию в приложениях, установленных на хромбуке, чтобы приложения запомнили это устройство. Завершив свои банковские и медицинские дела, отложите хромбук до тех пор, пока вам снова не понадобится проверить баланс счета или записаться на прием к врачу.

Может показаться, что все это — дополнительные сложности. Так и есть. Вместо постоянного доступа к своей банковской информации вы получаете почти постоянный доступ. Но зато вы в разы уменьшите вероятность того, что кто-то воспользуется вашими банковскими данными. Если на хромбуке установлены только два или три приложения или в закладках у вас сохранена только страница банка или медицинского учреждения и вы не посещаете никакие другие сайты, опять же очень маловероятно, что кто-то украдет ваши данные с помощью трояна или другого вредоносного программного обеспечения.

Итак, мы поговорили о том, как создать надежный пароль и сохранить его в тайне. Везде, где только возможно, включайте двухфакторную аутентификацию. Несколько следующих глав посвящены тому, какие следы вы оставляете, занимаясь повседневными рутинными делами, и как сохранить конфиденциальность.

Глава 2

КТО ЕЩЕ ЧИТАЕТ ВАШУ ЭЛЕКТРОННУЮ ПОЧТУ?

Если мы с вами похожи, то едва ли не первое, что вы делаете утром, — это проверяете электронную почту. И, если мы с вами похожи, вам тоже интересно, кто еще мог прочитать ее. Паранойя тут ни при чем. Если вы пользуетесь такими службами, как Gmail или Outlook 365, ответ довольно очевидный и пугающий.

Даже если вы удалили электронное письмо сразу же, как прочитали его на компьютере или смартфоне, это вовсе не значит, что вы уничтожили его бесследно. Где-то все равно существует копия. Веб-почта основана на использовании облачных технологий, поэтому, чтобы вы могли войти в нее с любого устройства, из любой точки мира и в любое время, обязательно должны существовать резервные копии всех писем. Например, если вы пользуетесь сервисом Gmail, копия каждого письма, которое вы отправляете или получаете через свою учетную запись, сохраняется на различных серверах Google по всему миру. То же самое относится и к почтовым сервисам, предоставляемым компаниями Yahoo! Apple, AT&T, Comcast, Microsoft или даже фирмой, где вы работаете. Кроме того, в любой момент любое отправленное вами электронное письмо может подвергнуться проверке со стороны компании, предоставляющей хостинг. Утверждается, будто бы это способ избавить вас от спама, но в действительности третьи лица могут (и пользуются этой возможностью) читать наши письма по совершенно иным, гораздо более корыстным и низменным причинам.

В любой момент любое отправленное вами электронное письмо может подвергнуться проверке со стороны компании, предоставляющей хостинг. Утверждается, будто бы это способ избавить вас от спама, но в действительности третьи лица могут (и пользуются этой возможностью) читать наши письма по совершенно иным, гораздо более корыстным и низменным причинам.

В принципе, большинство из нас никогда не станет оправдывать того, кто читает чужие электронные письма. Существуют законы, защищающие бумажные письма, которые были отправлены через почтовую службу

США, и подобные законы для электронной корреспонденции. И все же на практике мы, как правило, понимаем и, вероятно, соглашаемся с тем, что за простоту общения по электронной почте приходится чем-то расплачиваться. Мы знаем, что Yahoo! (как и другие компании) предоставляет бесплатный сервис электронной почты, и мы знаем, что основную часть своей прибыли Yahoo! получает от рекламы. Вероятно, мы не осознаем, насколько тесно эти вещи могут быть связаны между собой и как все это может повлиять на неприкосновенность нашей частной жизни.

Но однажды это вдруг понял житель Северной Каролины Стюарт Даймонд. Он осознал, что реклама, отображавшаяся в верхнем правом углу страницы его учетной записи почтового сервиса Yahoo! не была случайной. Рекламные объявления соответствовали тексту электронных писем, которые он отправлял или получал. Например, если в письме упоминалась планируемая деловая поездка в Дубай, в рекламе, отображающейся в учетной записи, выводилась информация об авиакомпаниях, отелях и развлечениях в ОАЭ.

Обычно все подобные вещи подробно прописаны в тексте пользовательского соглашения, условия которого большинство из нас принимает, не читая. Никто не хочет видеть рекламу, не имеющую никакого отношения к его личным интересам, верно же? И когда дело касается переписки между пользователями почтовой службы Yahoo! кажется вполне логичным, что компания сможет просканировать текст этих писем и настроить рекламу в соответствии с нашими потребностями, а также, может быть, отфильтровать спам.

Однако Даймонд, а также некий Дэвид Саттон, тоже житель Северной Каролины, стали замечать, что на подборку рекламы влияло содержимое не только писем, отправленных и полученных с других аккаунтов в почтовом сервисе Yahoo! но и писем, отправителями или получателями которых были владельцы учетных записей и на *других сервисах*. Из этого следовал вывод, что компания перехватывала и читала всю почту, а не только ту, которая перемещалась между ее собственными серверами.

Опираясь на собственные наблюдения, в 2012 году они подали против компании Yahoo! коллективный иск от лица 275 миллионов пользователей, обеспокоенных тем, что компания фактически занимается шпионажем в обход всех законов.

Изменилось ли что-нибудь после этого? Нет.

Когда дело касается коллективного иска, обеим сторонам дается время на то, чтобы прояснить все обстоятельства и представить свой ответ. В данном случае этот период продлился почти три года. В июне 2015 года судья в городе Сан-Хосе, штат Калифорния, вынес решение, что истцы предоставили достаточные основания для того, чтобы дать делу ход, и что люди, отправлявшие или

получавшие письма с помощью почтового сервиса Yahoo! со 2 октября 2012 года, когда был подан первоначальный иск, могли присоединиться к коллективному иску на основании закона «О сохраненных сообщениях» (Stored Communications Act). Кроме того, ряд проживающих в Калифорнии пользователей других почтовых сервисов также получили право присоединиться к иску в соответствии с законом штата «О вторжении в личную жизнь» (Invasion of Privacy Act). Судебная тяжба по этому делу все еще идет.

Компания Google, против которой также подали иск за просмотр электронных писем еще в 2014 году, во время судебного заседания случайно сделала достоянием гласности тот факт, что она в самом деле читает пользовательские письма, а затем сразу же постаралась скрыть или изъять эти данные, но безуспешно. В деле всплыл вопрос о том, что именно сканировала или читала компания Google. Согласно показаниям истцов, в число которых входило несколько крупных медиакорпораций, например владельцы газеты USA Today, компания Google в какой-то момент поняла, что, просматривая содержимое лишь входящих писем, можно упустить множество полезных сведений. Истцы утверждали, что компания Google перешла от изучения содержимого только заархивированных писем, которые хранятся на сервере Google, к проверке всей почты в учетной записи Gmail, будь то письма, отправленные со смартфона iPhone или же с ноутбука, используемого в кофейне.

Иногда компании даже пытались тайно просматривать письма, преследуя собственные интересы. Один из наиболее известных подобных случаев связан с корпорацией Microsoft, на которую обрушилась волна общественного гнева, когда выяснилось, что она просматривала содержимое входящих писем одного из пользователей сервиса Hotmail, который, как подозревалось, был обладателем пиратской копии программного обеспечения Microsoft. В результате этого открытия корпорация Microsoft заявила, что в дальнейшем подобными расследованиями будут заниматься органы правопорядка.

Подобные случаи не ограничиваются частной электронной почтой. Если вы отправите письмо с рабочего ящика, IT-отдел компании, в которой вы работаете, также сможет просмотреть и сохранить его в своем архиве. И уже персонал или руководство IT-отдела будет решать, пропустить ли помеченное электронное письмо через свой сервер или же обратиться в правоохранительные органы. В группу риска попадают письма, содержащие коммерческие тайны или сомнительные материалы, например порнографию. Также письма проверяются на спам. Если IT-отдел просматривает и сохраняет ваши письма, каждый раз при входе в систему вы должны получать напоминание о действующей политике — хотя многие компании этого не делают.

Хотя большинство из нас может смириться с тем, что письма просматриваются на предмет спама, и, вероятно, некоторые из нас готовы закрыть глаза на просматривание своей почты в рекламных целях, сама мысль о том, что посторонние лица читают наши письма и действуют исходя из их содержимого, вызывает неприятные эмоции. (Конечно, если речь не идет о детской порнографии.)

Поэтому, когда вы пишете электронное письмо, пусть даже совсем незначительное, пусть даже вы его удалили из ящика, помните, что, вполне вероятно, текст и изображения из него будут просмотрены и сохранены, может, и не навсегда, но на довольно длительное время.

Поэтому, когда вы пишете электронное письмо, пусть даже совсем незначительное, пусть даже вы его удалили из ящика, помните, что, вполне вероятно, текст и изображения из него будут просмотрены и сохранены, может, и не навсегда, но на довольно длительное время. (Некоторые компании хранят эти материалы дольше, некоторые — более короткое время, но лучше исходить из того, что большинство компаний хранят письма довольно долго.)

Теперь, когда вам известно, что правительство и корпорации читают ваши письма, самое малое, что вы можете сделать, — это максимально усложнить им задачу.

Чтобы стать невидимым, вам необходимо будет зашифровать свое сообщение, чтобы только получатель мог разблокировать и прочитать содержимое.

Большинство сервисов веб-почты применяют шифрование, когда письмо пересылается с одного ящика на другой. Однако когда некоторые сервисы пересылают письмо между почтовыми серверами (агентами пересылки сообщений, MTA), они могут не пользоваться шифрованием, а значит, ваше письмо будет не защищено. Например, на работе у начальника может быть доступ ко всей корпоративной почте. Чтобы стать невидимым, вам необходимо будет зашифровать свое сообщение, чтобы только получатель мог разблокировать и прочитать содержимое. Что такое шифрование? Это код.

Очень простой пример шифрования (например, шифр Цезаря) — это когда каждая буква заменяется другой, расположенной в алфавите на определенном расстоянии от исходной буквы. Например, если это расстояние составляет две буквы, то с помощью кода Цезаря А превращается в В, В превращается в Д, Я превращается в Б, и так далее. С помощью этой системы шифрования имя Кевин Митник пишется как «Мждкп Окфпкм».

Сейчас большинство систем шифрования, конечно, гораздо сложнее шифра Цезаря. Поэтому их гораздо сложнее взломать. Но абсолютно все виды шифров объединяет то, что во всех них используется ключ — своего рода пароль, с помощью которого можно расшифровать и прочитать закодированное послание. При симметричном шифровании один и тот же ключ применяется как для зашифровывания, так и для расшифровывания сообщений. Однако симметричные шифры сложнее применять, когда две стороны незнакомы друг с другом или находятся далеко друг от друга, как часто бывает при общении через Интернет.

В большинстве инструментов для шифрования электронной почты используется так называемое асимметричное шифрование. Это означает, что генерируются два ключа: один — закрытый ключ (которым я не делюсь ни с кем, он хранится только на моем устройстве), а второй — открытый (который я выкладываю в Интернет в открытый доступ). Ключи разные, но они связаны между собой математически.

Например, Боб хочет отправить Алисе защищенное электронное письмо. Он находит в Интернете открытый ключ Алисы или получает его от Алисы напрямую и при отправке сообщения шифрует его с помощью ее ключа. Это сообщение будет зашифровано до тех пор, пока Алиса — и никто другой — не расшифрует его с помощью своего закрытого ключа.

Так что же необходимо для шифрования содержимого своих электронных писем?

Самый популярный метод шифрования электронной почты — это плагин PGP (полное название — Pretty Good Privacy). Он не бесплатен. Это продукт компании Symantec Corporation. Но его создатель, Фил Циммерман, также разработал и его бесплатную версию, OpenPGP, которая находится в открытом доступе. И третий вариант — программа GnuPG (GNU Privacy Guard), созданная Вернером Кохом, которая также бесплатна. Хорошо то, что все три программы взаимозаменяемы. Иными словами, не важно, какой версией PGP вы пользуетесь, поскольку основные функции одинаковы во всех трех программах.

Когда Эвард Сноуден решил впервые предать огласке секретные документы АНБ, ему понадобилась помощь и поддержка единомышленников по всему миру. Как ни парадоксально, ему нужно было выбраться из Интернета, оставаясь при этом его активным пользователем. Ему необходимо было стать невидимым.

Даже если вы не собираетесь разглашать государственные тайны, вы, вероятно, все равно хотите, чтобы ваша переписка в Интернете была конфиденциальна. Как показывает пример Сноудена и многих других людей, добиться этого нелегко, но при должном усердии возможно.

У Сноудена был личный аккаунт на сервисе Lavabit, с помощью которого он общался с другими людьми. Но для отправки электронной почты используется не двухточечный протокол, т. е. одно письмо может пройти через несколько серверов по всему миру, прежде чем окажется в папке «Входящие» почтового ящика непосредственного получателя. Сноуден знал, что все написанное им может быть прочитано любым человеком, перехватившим письмо в любой точке этого маршрута.

Поэтому, чтобы создать действительно безопасный, анонимный и полностью зашифрованный канал связи с Лорой Пойтрас, кинорежиссером и защитницей права на неприкосновенность частной жизни, Сноудену пришлось совершить непростой маневр. Пойтрас к тому моменту только что завершила работу над документальным фильмом о разоблачителях. Сноуден хотел общаться с Пойтрас с помощью защищенных писем, но только несколько людей знали ее открытый ключ. Ее открытый ключ оказался далеко не таким уж открытым.

Чтобы найти ее открытый ключ, Сноудену пришлось обратиться за помощью к человеку по имени Мика Ли из Фонда электронных рубежей (англ. Electronic Frontier Foundation, EFF), который занимается защитой права на неприкосновенность частной жизни в Интернете. Открытый ключ Ли находился в свободном доступе в Интернете, и, согласно обзору, опубликованному в интернет-издании The Intercept, ему также был известен открытый ключ Пойтрас, но сначала ему нужно было связаться с ней и убедиться, что она согласна сообщить его Сноудену. Она согласилась.

В этот момент ни Ли, ни Пойтрас не знали, кому именно понадобился открытый ключ Лоры, знали только, что понадобился *кому-то*. Для связи Сноуден использовал не личный электронный ящик. Однако если вы редко пользуетесь PGP-шифрованием, вы можете время от времени забывать зашифровать важное электронное письмо, что и произошло с самим Сноуденом. Он забыл указать в письме свой открытый ключ, с помощью которого Ли мог бы ему ответить.

Не имея возможности безопасно связаться с таинственным незнакомцем, Ли был вынужден отправить обычное, незашифрованное ответное письмо, в котором попросил Сноудена сообщить ему свой открытый ключ, что тот и сделал.

Ли, доверенному третьему лицу, снова пришлось вмешаться. По личному опыту могу сказать вам, что очень важно точно установить личность человека, с которым вы обмениваетесь защищенными

письмами, и желательно сделать это через общего друга, а также убедиться, что вы переписываетесь именно с этим другом, а не с кем-то еще, выдающим себя за него.

Я не понаслышке знаю о том, как это важно: раньше я часто оказывался в ситуации, когда другая сторона не сомневалась в том, что я именно тот, кем представляюсь, и не перепроверяла мой открытый ключ — и это было мне на руку. Как-то раз я хотел пообщаться с Нилом Клифтом, магистрантом в Университете Лидса в Англии, изучавшим органическую химию. Нил замечательно справлялся с поиском уязвимостей в операционной системе VMS компании Digital Equipment Corporation (DEC). Я хотел, чтобы Клифт отправил мне список всех обнаруженных им брешей в системе безопасности, о которых он сообщил в компанию DEC. Для этого мне нужно было, чтобы он считал меня одним из сотрудников DEC.

Сначала я отправил Клифту сфабрикованное сообщение от имени некого Дейва Хатчинса. До этого я позвонил Клифту, представившись Дерреллом Пайпером из компании VMS Engineering, поэтому я (притворяясь Хатчинсом) написал в письме, что Пайпер хотел по электронной почте обсудить с Клифтом проект. Прошерстив систему электронной почты компании DEC, я знал, что Клифт и настоящий Пайпер уже переписывались ранее, поэтому мое предложение не казалось таким уж странным. Затем я отправил письмо с настоящего ящика Пайпера.

Чтобы окончательно усыпить бдительность Клифта, я даже предложил ему пользоваться PGP-шифрованием, чтобы какой-нибудь Кевин Митник не смог прочитать письма. Вскоре Клифт и «Пайпер» обменялись открытыми ключами и зашифровали свою переписку — переписку, которую я, как Пайпер, мог читать. Ошибкой Клифта было то, что он не усомнился в личности самого Пайпера. Как в ситуации, когда вам внезапно звонят из банка и спрашивают паспортные данные или номер счета, вы всегда должны повесить трубку и самостоятельно перезвонить в банк — никогда нельзя быть уверенным, с кем разговариваешь или переписываешься.

Принимая во внимание важность секретной информации, о которой шла речь, Сноуден и Пойтрас не могли пользоваться своими личными адресами электронной почты. Почему? Личные электронные ящики были связаны с уникальным набором данных — например, интересы, список контактов, — по которым можно было вычислить каждого из них. Сноуден и Пойтрас решили завести новые электронные ящики.

Единственной проблемой было то, как передать друг другу эти новые электронные адреса? Другими словами, если обе стороны стали полностью анонимными, откуда они могли знать, кто есть кто и кому можно доверять? Как Сноуден, например, мог быть уверен, что АНБ или кто-нибудь другой не выдает себя за Пойтрас? Открытый ключ состоит из множества символов, поэтому нельзя просто взять телефон, позвонить по защищенной линии и продиктовать его другому человеку. Необходим безопасный электронный ящик.

Мика Ли снова оказался вовлечен в ситуацию, он стал доверенным связующим звеном между Сноуденом и Пойтрас, пока те создавали новые анонимные электронные ящики. Пойтрас первая передала Ли свой новый открытый ключ. Но ключи для PGP-шифрования очень длинные (конечно, не как число Пи, но все же), и, что если кто-то читает письма самого Ли? Поэтому вместо целого ключа Ли взял его идентификатор (отпечаток), состоящий из 40 символов. И выложил его в открытый доступ, в Twitter.

Иногда, чтобы стать невидимым, приходится быть на виду.

Теперь Сноуден мог анонимно просмотреть Twitter Ли и сверить сокращенный ключ с полученным сообщением. Если бы они не совпадали, Сноуден понял бы, что письмо нельзя открывать. Оно могло быть взломано. Или его мог отправить кто-то из АНБ.

В этом случае ключи совпали.

Теперь, на несколько шагов отодвинувшись от того, кем они были в Интернете — и в реальном мире, — Сноуден и Пойтрас были почти готовы начать свою тайную, защищенную и анонимную электронную переписку.

Сноуден наконец отправил Пойтрас зашифрованное письмо, в котором подписался как «Гражданин четыре» (Citizen Four). Этот псевдоним стал названием снятого Лорой Пойтрас оскароносного документального фильма о борьбе Сноудена за право на конфиденциальность.

Возможно, кто-то подумает, что на этом все и закончилось — теперь они могли спокойно общаться с помощью зашифрованных писем, но это не так. Это было всего лишь начало.

На волне террористических актов в Париже в 2015 году правительства нескольких стран обсуждали инструменты обхода подобных систем защиты или другие методы, с помощью которых чиновники могли бы расшифровывать закодированные электронные письма, текстовые сообщения или SMS — якобы защищаясь от иностранных террористов. Конечно, это противоречит самой сути и предназначению шифрования. Однако, как вы увидите далее, правительствам на самом деле не

нужно видеть содержимое ваших писем, чтобы знать, с кем и как часто вы общаетесь.

Как я уже говорил ранее, зашифровать — значит закодировать сообщение так, чтобы раскодировать его мог только человек, который знает ключ. То, насколько легко человек без ключа сможет взломать ваш код, зависит и от сложности математической операции, и от длины самого ключа шифрования.

Распространенные сегодня алгоритмы шифрования общедоступны. Это хорошо. Бойтесь закрытых, не общедоступных алгоритмов шифрования. Общедоступные алгоритмы прошли проверку на слабые места — в том смысле, что люди намеренно пытались взломать их.

Когда в одном из общедоступных алгоритмов появляются уязвимости или его взламывают, он остается в прошлом и вместо него появляются новые, более надежные алгоритмы. Устаревшие алгоритмы никуда не исчезают, но пользоваться ими настоятельно не рекомендуется.

Ключи (в той или иной степени) являются зоной вашего контроля, поэтому, как вы могли догадаться, очень важно следить за ними. Если вы генерируете ключ шифрования, вы — и только вы — будете хранить этот ключ на своем устройстве. Если вы поручите шифрование какой-нибудь компании, например, через облачный сервис, то она сможет сохранить у себя ваш ключ. Главная причина для беспокойства заключается в том, что по закону эта компания может быть обязана передавать ваш ключ органам правопорядка или спецслужбам, при этом вас могут не поставить в известность о происходящем. Вам нужно читать политику конфиденциальности каждого сервиса, которым вы пользуетесь для шифрования, чтобы понимать, у кого будут ваши ключи.

Когда вы зашифровываете сообщение — электронное письмо, текстовое сообщение или телефонные переговоры, — предпочтительно сквозное (оконечное) шифрование. При этом ваше сообщение невозможно будет прочитать до тех пор, пока оно не дойдет до своего адресата. При сквозном шифровании только у вас и у получателя будут ключи, с помощью которых расшифровывается послание. Никто, кроме вас, не сможет этого сделать — ни телекоммуникационная компания, ни владелец веб-сайта, ни разработчик приложения — т. е. никто из тех, к кому обращаются органы правопорядка или спецслужбы, чтобы получить информацию о вас. Как узнать, использует ли выбранный вами сервис сквозное шифрование? Введите в поисковой строке Google запрос «почтовая служба со сквозным шифрованием». Выбрав сервис, проверьте, чтобы генерируемые ключи сохранялись только на вашем устройстве и на устройстве получателя и больше нигде. Если на сайте об этом не говорится, ищите другой.

Если все это кажется вам сложным, то только потому, что так оно и есть. Но существуют специальные PGP-плагины для браузеров Chrome и Firefox, которые значительно упрощают процесс шифрования. Один из них, под названием Mailvelope, отлично справляется с созданием и хранением открытых и закрытых ключей шифрования PGP. Просто напечатайте кодовую фразу, на основе которой генерируются открытый и закрытый ключи. Затем, когда в следующий раз вы будете писать письмо, пользуясь веб-почтой, выберите получателя, и, зная его открытый ключ, вы сможете отправить ему зашифрованное письмо.

Даже если вы шифруете свои электронные письма с помощью PGP, небольшую, но очень информативную часть вашей почты все равно может прочитать кто угодно. Пытаясь защититься от разоблачительных заявлений Сноудена, правительство США снова и снова твердило, что не занимается перехватом фактического содержимого электронной почты, которое при PGP-шифровании прочитать невозможно. Вместо этого правительство заявляло о том, что оно собирает только метаданные.

Что собой представляют метаданные электронной почты? Это значения полей «кому», «от кого» и адреса всех серверов, через которые проходило письмо по пути от отправителя к получателю. Также сюда входит строка с темой письма, которая иногда может очень многое сказать о его зашифрованном содержимом. Метаданные, пережиток ранних этапов развития Интернета, до сих пор являются частью каждого электронного письма, но в современных почтовых сервисах эта информация скрыта.

Какой бы плагин PGP вы ни выбрали, программа не шифрует метаданные — информацию в полях «кому» и «от кого», а также дату отправления. Все это останется в виде открытого текста, независимо от того, видите вы эти данные или нет.

Какой бы плагин PGP вы ни выбрали, программа не шифрует метаданные — информацию в полях «кому» и «от кого», а также дату отправления. Все это останется в виде открытого текста, независимо от того, видите вы эти данные или нет. Посторонние лица смогут прочитать метаданные зашифрованного послания, и они узнают, что такого-то числа вы отправили письмо такому-то получателю, а через два дня — снова, и так далее.

Может быть, в этом нет ничего страшного, поскольку эти посторонние люди не смогут прочитать, что именно вы написали, и вам, вероятно, не представляются важными технические детали

пересылки письма, через какие серверы и в какое время оно проходило, но вы удивитесь, как много можно узнать только на основании маршрута писем и частоты их отправления.

Еще в 90-е, до того как я пустился в бега от ФБР, я занимался так называемым «анализом метаданных» распечаток телефонных соединений. Сначала я взломал сервер PacTel Cellular, оператора сотовой связи в Лос-Анджелесе, и получил полную детализацию соединений всех, кто разговаривал по телефону с информатором, от которого ФБР получало сведения обо мне и моих действиях.

Детализация соединений очень напоминает метаданные, о которых мы говорили ранее. Там отмечено время соединения, набранный номер, длительность соединения, а также сколько раз звонили с того или иного номера, все это очень важно.

Просмотрев все вызовы, совершенные с помощью оператора PacTel Cellular на городской номер информатора, я сумел составить список мобильных номеров всех людей, которые ему звонили. Проанализировав биллинговую информацию звонивших, я смог определить, что они были сотрудниками ФБР и совершали вызовы из офиса Бюро в Лос-Анджелесе. Вполне очевидно, что некоторые из набранных этими людьми номеров принадлежали офису ФБР в Лос-Анджелесе, прокуратуре США и другим государственным структурам. Некоторые вызовы были очень длительными. На некоторые номера звонили очень часто.

Когда информатора переселяли в новое безопасное место, я узнавал его городской номер телефона, поскольку агенты звонили туда, если им не удавалось связаться с информатором по пейджеру. Получив номер телефона информатора, я посредством социальной инженерии легко определял адрес дома — я притворялся сотрудником телекоммуникационной компании Pacific Bell, обслуживавшей этот район.

Социальная инженерия — это метод несанкционированного доступа к информации путем психологического воздействия, манипулирования и управления действиями человека с целью заставить его выполнить желаемое. Часто из человека обманным путем выуживают конфиденциальную информацию. В данном случае мне были известны служебные номера телефонной компании, и я, представившись техническим специалистом на выезде, оперировал соответствующей ситуации терминологией и профессиональной лексикой, чтобы получить от компании конфиденциальные сведения.

Поэтому хотя отслеживание и хранение метаданных электронной почты — это не то же самое, что перехват фактического содержимого писем, но это все равно можно рассматривать как вторжение в частную жизнь.

Если вы посмотрите на метаданные одного из недавно полученных писем, вы увидите IP-адреса тех серверов, которые служили передаточными пунктами для вашего письма по всему миру, пока оно шло к адресату. У каждого сервера — как и у каждого человека, пользующегося Интернетом — есть уникальный IP-адрес, числовая величина, которая зависит от страны вашего пребывания и от интернет-провайдера. За каждой страной закреплен свой блок IP-адресов. Разным частям мира присвоены целые блоки IP-адресов, и за каждым провайдером зарезервирован собственный подблок, который в свою очередь делится на подблоки в зависимости от типа предоставляемых услуг: коммутируемый доступ, выделенная линия или мобильный Интернет. Если вы приобрели статический IP-адрес, он будет привязан к вашей учетной записи и к домашнему адресу, в противном случае ваш внешний IP-адрес будет генерироваться из пула адресов, принадлежащих вашему интернет-провайдеру. Так, например, обладатель IP-адреса 27.126.148.104 находится в Виктории, Австралия.

Или, например, IP-адрес 175.45.176.0 принадлежит Северной Корее. Письмо от отправителя с таким IP-адресом, вероятно, будет помечено для дальнейшего изучения. Кто-нибудь из правительства США, возможно, пожелает узнать, почему вы переписываетесь с человеком из Северной Кореи, даже если в теме письма будет написано «С днем рождения».

Возможно, сам по себе адрес сервера не так уж интересен. Но частота взаимодействия с ним может многое рассказать. Кроме того, если вы определите каждый элемент, отправителя, получателя и их местонахождение, вы начнете понимать, что происходит на самом деле. Например, метаданные телефонных соединений, текстовых сообщений и электронных писем — их частота, время суток и пр. — могут многое рассказать о душевном здоровье человека.

Звонок в 22 часа на горячую линию для жертв домашнего насилия длительностью 10 минут или вызов в полночь с Бруклинского моста на горячую линию по предотвращению самоубийств длительностью 20 минут говорят о многом. В Дартмутском колледже разработали приложение, которое распознает в пользовательских данных шаблоны поведения, характерные для людей, испытывающих стресс, депрессию и одиночество. Также изучается взаимосвязь между подобным поведением и академической успеваемостью студента.

Все еще не видите ничего страшного в том, чтобы метаданные ваших электронных писем находились в открытом доступе? В Массачусетском технологическом институте был разработан проект под названием Immersion (Погружение). Это программа, которая позволяет на основе одних лишь метаданных создать наглядную схему взаимоотношений между отправителями и получателями всех писем, хранящихся в вашем аккаунте Gmail. Инструмент наглядно демонстрирует, кто из адресатов для вас наиболее важен. Программа даже выводит шкалу времени, чтобы было видно, как знакомые вам люди с течением времени обретали или теряли значимость в вашей жизни. Хотя, вероятно, вам кажется, что тут все и так понятно, но визуальное отображение этих взаимосвязей может на многое открыть вам глаза. Вполне возможно, что вы и не представляли себе, как часто отправляете электронные письма практически незнакомому человеку и как редко человеку, которого очень хорошо знаете. Как бы то ни было, инструмент Immersion дает вам возможность самостоятельно решать, загружать ли в него данные, а также удалить информацию после составления графика.

Если верить Сноудену, АНБ и другие агентства хранят метаданные наших электронных писем, текстовых сообщений и телефонных соединений. Но не может же правительство хранить метаданные абсолютно каждого человека. Или может? Технически — нет. Однако, начиная с 2001 года, в «законном» сборе информации произошли существенные изменения.

В соответствии с принятым в США в 1978 году Актом о негласном наблюдении в целях внешней разведки (англ. Foreign Intelligence Surveillance Act, FISA), все запросы на выдачу разрешения на наблюдение за иностранными гражданами на территории США рассматривает Суд по наблюдению в целях разведки (англ. Foreign Intelligence Surveillance Court). Казалось бы, вполне логично, что между человеком и правоохранительными органами должен стоять судебный ордер. В действительности все происходит несколько иначе. Только в 2012 году из поступивших в суд 1856 запросов на слежку было одобрено 1856, из чего напрашивается вывод, что выдача ордеров для правительства США превратилась по большому счету в простую формальность. После того как Суд по наблюдению в целях разведки одобряет запрос, правоохранительные органы могут потребовать от частных корпораций выдать все имеющиеся у них данные о вас — если они, конечно, не сделали этого ранее.

Чтобы стать по-настоящему невидимым в цифровом мире, недостаточно просто шифровать сообщения. Также нужно:

Скрывать свой настоящий IP-адрес — то есть точку выхода в Интернет, ваш след. Он может выдать ваше местоположение (вплоть до конкретного адреса) и вашего интернет-провайдера.

Стирать данные о своем программном и аппаратном обеспечении — когда вы выходите в Интернет, на сайт отправляется отчет об используемом вами программном обеспечении и аппаратных средствах. Определить, какое именно программное обеспечение установлено, можно с помощью различных технологий, таких как Adobe Flash. Браузер передает сайту сведения о том, какая версия операционной системы у вас установлена, а иногда также о том, каким еще программным обеспечением вы пользуетесь на своем компьютере.

Оберегать свою анонимность — идентифицировать личность в Интернете очень трудно. Доказать, что именно вы были за компьютером, когда что-то случилось, довольно сложно. Однако если вы прошлись перед камерой прежде, чем выйти в Интернет из кофейни Starbucks, или если вы просто купили там латте, расплатившись своей картой, все это может указать на то, что вы вышли в Интернет через несколько минут после вышеописанных событий.

Как мы уже выяснили, при каждом подключении к Интернету вам приписывается определенный адрес. Это проблема, если вы хотите быть невидимым в Интернете: вы можете изменить имя (или вообще его не указывать), но IP-адрес все равно выдаст ваше местонахождение на нашей планете, вашего интернет-провайдера и человека, который платит за доступ в Интернет (это можете быть вы или кто-то другой). Все эти фрагменты информации присутствуют в метаданных электронного письма, и впоследствии с их помощью вас можно будет идентифицировать. Любое общение, будь то электронная переписка или что-то другое, может способствовать идентификации вашей личности через IP-адрес, который приписан к тому маршрутизатору, которым вы пользуетесь дома, на работе или у друзей.

IP-адреса в электронных письмах, безусловно, можно подделать. Некоторые пользуются прокси-серверами — заменяют свой реальный IP-адрес чьим-то другим, — поэтому кажется, что их электронные письма отправлены из какого-то другого места. Прокси-сервер — это как переводчик с иностранного языка: вы говорите с переводчиком, а тот говорит с иностранцем, только в случае с прокси-сервером сообщение передается в абсолютно неизменном виде. Суть в том, что с помощью прокси-сервера можно скрыть, что в действительности письмо отправлено не из Китая или Германии, а из Северной Кореи.

Вместо создания и администрирования собственного прокси-сервера можно пользоваться таким типом сервисов, как анонимные ремейлеры — они скроют реальный IP-адрес, с которого вы

отправляете электронные письма. Анонимный ремейлер просто меняет адрес электронной почты отправителя перед отправкой письма. Получатель может ответить также с помощью ремейлера. Это самый простой вариант.

Существуют и другие схемы. С помощью некоторых ремейлеров первого и второго типа нельзя отвечать на письма, можно только отправлять. Ремейлеры третьего типа, или Mixminion, позволяют и отвечать, и пересылать, и шифровать письма. Если вы собираетесь пользоваться этим методом анонимной переписки, нужно выяснить, какими возможностями располагает ваш ремейлер.

Один из способов маскировки IP-адреса заключается в использовании луковой маршрутизации (Tor), именно этот способ и выбрали Сноуден с Пойтрас.

Это программное обеспечение с открытым исходным кодом было разработано Военно-морской академией США в 2004 году, чтобы военнослужащие могли проводить свои исследования, не раскрывая своего местонахождения, и позже было доработано. Tor предназначается для людей, живущих в странах с авторитарным режимом и стремящихся обойти цензуру в общедоступных СМИ и сервисах, а также скрыть свои поисковые запросы. Tor — это бесплатное программное обеспечение, которым может пользоваться кто угодно и где угодно, в том числе вы.

Как же работает Tor? Система принципиально поменяла модель доступа к сайту.

Обычно, когда вы выходите в Интернет, вы запускаете веб-браузер и вводите адрес нужного сайта. На сайт отправляется запрос, и через миллисекунду ваш браузер получает ответ и запрошенную страницу. Веб-сайт узнает — с помощью IP-адреса, — кто ваш интернет-провайдер, а иногда даже из какой точки мира вы выходите в Интернет (опираясь на то, где физически расположен ваш интернет-провайдер, или по количеству и частоте передачи пакетов с вашего устройства на сайт). Например, если ваше устройство заявляет, что находится в США, но время и скорость передачи данных свидетельствуют о том, что вы находитесь в какой-то другой точке мира, некоторые сайты — в частности игровые — расценят это как попытку мошенничества.

При использовании Tor непосредственное соединение между вами и целевым веб-сайтом скрывается за счет использования дополнительных узлов и каждые 30 секунд цепочка узлов, связывающая вас с тем сайтом, который вы просматриваете, меняется, не причиняя вам никаких неудобств. Множество узлов, соединяющих вас с сайтом — это слои, как в луковице. Иначе говоря, если бы кто-нибудь попытался отследить вас через просматриваемый веб-сайт, ему бы это не удалось, поскольку маршрут постоянно меняется. Если между вашей точкой входа и точкой выхода не будет каким-либо образом обнаружена связь, ваше соединение можно считать анонимным.

Когда вы выходите в Сеть через Tor, ваш запрос на загрузку страницы, например mitnicksecurity.com, отправляется не напрямую на соответствующий сервер, а на другой узел Tor. И, чтобы еще больше все запутать, этот узел передает запрос следующему узлу, который уже направляет его на mitnicksecurity.com. Таким образом, у нас есть входной узел, узел посередине и выходной узел. Если бы мне нужно было посмотреть, кто заходил на сайт моей компании, я бы смог увидеть только IP-адрес выходного узла, последнего в этой цепочке, а не первого, вашего входного узла. Можно настроить Tor Browser таким образом, чтобы он пользовался выходными узлами в определенной стране, например в Испании, или даже каким-то конкретным выходным узлом, например в Гонолулу.

Чтобы пользоваться Tor, необходим специально доработанный браузер Firefox, который можно скачать с сайта Tor (torproject.org). Всегда устанавливайте специализированный Tor Browser для своей операционной системы с официального сайта Tor Project. Не выходите в Сеть через браузеры сторонних разработчиков. Для операционной системы Android можно скачать из Google Play бесплатное официальное приложение для выхода в Tor — Orbot, которое как шифрует ваш трафик, так и скрывает IP-адрес. Для устройств под управлением операционной системы iOS (iPad, iPhone) существует Onion Browser, официальное приложение, доступное в iTunes App Store.

Возможно, вы подумали, почему бы просто не создать сервер электронной почты непосредственно в сети Tor? Он был создан — почтовый сервис Tor Mail с хостингом на сайте, доступ к которому был возможен только через Tor Browser. Однако ФБР, расследуя совершенно не связанное с анонимностью дело, получило ордер на доступ к хранящимся на нем данным и, следовательно, ко всем зашифрованным письмам на сервере Tor Mail. Эта поучительная история демонстрирует, что, даже если вы уверены в безопасности своей информации, вы можете ошибаться.

Хотя у Tor есть собственная сеть, технология позволяет выходить и в обычный Интернет, единственное, при этом страницы будут загружаться гораздо медленнее. Помимо доступа в обычный Интернет, Tor дает возможность погрузиться в мир сайтов, которые не найти через общедоступный поиск в Интернете. Этот мир называется Даркнет (или «скрытая сеть»). Это сайты, имена которых не соответствуют общепринятым шаблонам (например, Google.com), а оканчиваются — .onion. Через некоторые из этих скрытых сайтов предлагают, продают или предоставляют незаконные товары и услуги. Некоторыми из этих сайтов пользуются люди из стран с жестким

цензурным режимом.

Однако необходимо отметить, что у технологии Tor есть ряд уязвимостей:

• У вас отсутствует контроль над выходными узлами, любой из которых может оказаться в руках правительства или правоохранительных органов.

• За вами по-прежнему можно следить и даже установить вашу личность.

Tor работает очень медленно.

Если вы все-таки решите пользоваться Tor, не нужно запускать его на том же устройстве, с помощью которого вы обычно выходите в Интернет. Другими словами, пусть у вас будет ноутбук, с которого вы выходите в Интернет, и отдельное устройство только для Tor (например, мини-компьютер Raspberry Pi, на котором запускается программное обеспечение Tor). Суть в том, что, если кто-нибудь сможет получить доступ к вашему компьютеру, у него все равно не получится просмотреть ваш Tor-трафик, потому что для Tor у вас предназначено совершенно иное устройство.

В случае со Сноуденом и Пойтрас, как я уже говорил, недостаточно было просто связаться друг с другом по зашифрованной электронной почте. После того как Пойтрас создала новый открытый ключ для своего анонимного адреса электронной почты, она смогла бы отправить его на старый электронный ящик Сноудена, но если бы кто-то следил за этим ящиком, то ее новые данные были бы раскрыты. Главное правило тут заключается в том, что необходимо изолировать анонимные аккаунты от всего, что может хоть как-то раскрыть вашу личность.

Чтобы быть невидимым, с каждым новым человеком общение нужно начинать с чистого листа, если необходимо исключить вероятность утечки. Обычный электронный ящик может быть связан с различными аспектами вашей реальной жизни — друзьями, увлечениями, работой. Для конфиденциального общения необходимо создать новый электронный почтовый ящик через Tor, чтобы IP-адрес, с которого создается ящик, никак нельзя было привязать к вашей реальной личности.

Чтобы быть невидимым, с каждым новым человеком общение нужно начинать с чистого листа, если необходимо исключить вероятность утечки. Обычный электронный ящик может быть связан с различными аспектами вашей реальной жизни — друзьями, увлечениями, работой.

Создание анонимного электронного ящика — сложная, но выполнимая задача.

Существуют службы приватной электронной почты. Если вы будете платить за них, вы оставите свой след, поэтому предпочтительнее выбирать бесплатный веб-сервис. Небольшая оговорка: в настоящее время Gmail, Microsoft, Yahoo! и другие сервисы требуют указать номер телефона для подтверждения своей личности. Совершенно очевидно, что пользоваться своим реальным номером нельзя, поскольку он может вывести на ваше настоящее имя и адрес. Возможно, вам удастся привязать аккаунт к телефонному номеру Skype, поскольку теперь Gmail поддерживает голосовую верификацию вместо верификации по SMS-сообщению. Однако чтобы создать телефонный номер Skype, вам все равно будет нужен действующий адрес электронной почты и ваучер Skype. Если вы считаете, что ситуацию можно исправить с помощью предоплаченного мобильного телефона, вы ошибаетесь. Если вы когда-либо звонили с этого предоплаченного телефона по своим личным делам, вычислить вас проще, чем отобрать конфету у ребенка.

Вместо этого лучше пользоваться одноразовыми телефонами. Некоторые люди считают, что использование таких телефонов — это прерогатива террористов, сутенеров и наркодилеров, но существует множество ситуаций, когда они могут пригодиться законопослушным гражданам. В качестве примера можно привести журналистку, вынужденную перейти на одноразовые телефоны, когда нанятые компанией Hewlett Packard частные детективы стали тщательно изучать содержимое ее мусорного бака — таким образом корпорация пыталась найти источник утечки важнейшей информации о совете директоров. После того случая она общалась со своим источником только по одноразовому телефону.

Другой пример. Женщина, которая избегает общения с назойливым бывшим, может получить свой глоток свободы, переключившись на телефон, для общения по которому не нужно заключать договор, а следовательно, указывать учетную запись Google или Apple. Одноразовые телефоны обычно практически не позволяют пользоваться Интернетом. Как правило, с них можно звонить, писать и пользоваться электронной почтой, и большинству людей этого достаточно. Однако вы также сможете получать данные, поскольку вы сможете подключить этот одноразовый телефон к своему ноутбуку и с его помощью выходить в Интернет. (Я расскажу вам, как менять MAC-адрес вашего ноутбука, чтобы при каждом подключении одноразовый телефон считался новым устройством.)

Однако купить одноразовый телефон, сохраняя свою анонимность, довольно трудно. Вашу личность помогут установить действия, совершенные в реальном мире. Конечно, я могу зайти в гипермаркет,

заплатить за одноразовый телефон наличными и оплатить (опять же наличными) сто минут общения. Кто узнает? Что ж, много кто узнает.

Во-первых, как я попаду в гипермаркет? Поеду на машине Uber? Возьму такси? Все эти данные могут приобщить к делу.

Я могу поехать на своей машине, но опять же правоохранительные органы смогут вычислить меня благодаря установленным на общественных парковках автоматическим считывателям номерных знаков для выявления автомобилей, находящихся в розыске. Данные с автоматических считывателей могут быть приобщены к делу.

Даже если я отправлюсь в гипермаркет пешком, мое лицо попадет в объектив нескольких камер наблюдения уже в самом магазине, и это видео также может быть приобщено к делу.

Ладно, допустим, я отправлю за телефоном кого-то другого — незнакомого мне человека, например, заплачу бездомному прямо на месте. Он войдет и купит за наличные телефон и несколько пополняемых карт. Это самый безопасный способ. Вы можете встретиться с этим человеком позже за много километров от магазина. Так вы сможете физически дистанцироваться от места совершения покупки. В этой ситуации самое слабое звено — это сам человек, с которым вы договорились — насколько можно ему доверять? Если заплатить ему больше стоимости самого телефона, то, скорее всего, он выполнит свою часть уговора и передаст вам телефон.

Активировать одноразовый телефон можно, или позвонив в службу поддержки оператора сотовой связи, или через сайт. Если вы не хотите, чтобы разговор записывался «в целях контроля качества обслуживания», лучше активировать телефон через Интернет. Выходить в сеть через Tor, подключаясь к общедоступной беспроводной сети, сменив перед этим MAC-адрес — это минимальные меры предосторожности. Все сведения, которые вы указываете о себе на сайте, должны быть выдуманными. Вместо своего адреса укажите адрес какого-нибудь крупного отеля, который можно найти в Интернете. Придумайте дату рождения и PIN-код и запомните эти данные на случай, если вам придется в будущем обращаться в службу поддержки.

Некоторые сервисы электронной почты вообще не требуют прохождения каких-либо проверок, и, если вы не опасаетесь преследования со стороны властей, телефонные номера Skype отлично подойдут для регистрации аккаунта Google и прочих подобных вещей. Но в качестве наглядного примера того, как можно применить на практике все то, о чем шла речь выше, представим себе, что, скрыв свой IP-адрес с помощью Tor и создав новый анонимный аккаунт Gmail, вы купили новый одноразовый мобильный телефон, на который вам пришел код подтверждения от Google или поступил голосовой вызов. Теперь у вас появился аккаунт Gmail, который практически невозможно отследить. Итак, у нас есть анонимный почтовый ящик, созданный на основе знакомых и привычных сервисов. Мы можем отправлять с него достаточно защищенные электронные письма, IP-адрес которых благодаря Tor будет скрыт (хотя у вас и нет контроля над выходными узлами), а содержимое которых благодаря PGP-шифрованию никто, кроме адресата, не сумеет прочитать.

Обратите внимание, что, если вы хотите сохранить анонимность нового ящика, вы должны заходить в него только через Tor, чтобы ваш настоящий IP-адрес невозможно было связать с этой почтой. Более того, нельзя пользоваться интернет-поиском, пока вы не вышли из этого анонимного аккаунта Gmail, иначе вы можете случайно ввести поисковый запрос, который тем или иным образом укажет на вас в реальной жизни. Даже поиск прогноза погоды может выдать ваше местонахождение.

Как вы видите, чтобы стать невидимым и оставаться невидимым, необходима незаурядная самодисциплина и неусыпная бдительность. Но это разумная плата за невидимость.

Самый важный итог этой главы заключается в следующем: во-первых, следует знать обо всех способах, как заинтересованное лицо сможет вычислить вас, даже если вы приняли некоторые (но не все возможные) меры предосторожности, описанные мной. И если вы все же примете все эти меры предосторожности, знайте, что, когда пользуетесь анонимным аккаунтом, всегда необходимо сохранять бдительность. Без исключений.

Также не лишним будет напомнить, что огромную роль играет сквозное шифрование, благодаря которому, в отличие от обычного шифрования, сообщение невозможно прочитать, пока оно не будет получено адресатом. Сквозное шифрование пригодится и в других случаях — при шифровании телефонных разговоров и мгновенных сообщений, — о чем мы поговорим в следующих двух главах.

Глава 3

ОСНОВЫ ПРОСЛУШКИ

Каждый день вы тратите немыслимое количество часов, уставившись в экран смартфона: общаясь, отвечая на сообщения, сидя в Интернете. Но знаете ли вы, как на самом деле работает ваш сотовый телефон?

Сотовая связь, благодаря которой функционируют мобильные телефоны, беспроводная и обеспечивается вышками сотовой связи — *базовыми станциями*. Чтобы оставаться на связи, сотовые телефоны постоянно отправляют слабые маячковые сигналы на ближайшую к ним станцию или станции. Базовые станции передают ответный сигнал, уровень которого выражается в количестве «столбиков» на экране мобильного телефона — отсутствие «столбиков» означает отсутствие сигнала.

Чтобы хоть как-то сохранить конфиденциальность пользователя, в сигналах с сотового телефона используется так называемый международный идентификатор мобильного абонента (IMSI), последовательность цифр и букв, присвоенная SIM-карте. Это пережиток тех времен, когда операторы сотовой связи отслеживали ближайшие к вам базовые станции, чтобы знать, пользовались ли вы станцией своего оператора или находились в роуминге (пользовались станцией другого оператора). Первый фрагмент кода IMSI содержит информацию о вашем мобильном операторе, а остальная его часть — это уникальный идентификатор вашего мобильного телефона в этой сотовой сети.

Каждый день вы тратите немыслимое количество часов, уставившись в экран смартфона: общаясь, отвечая на сообщения, сидя в Интернете. Но знаете ли вы, как на самом деле работает ваш сотовый телефон?

Правоохранительные органы создали устройства, которые выдают себя за базовые станции сотовой связи. Они разработаны для перехвата разговоров и текстовых сообщений. В США правоохранительные органы также пользуются устройствами, с помощью которых можно определить IMSI мобильного телефона. Он перехватывается менее чем за секунду и без каких-либо уведомлений. Как правило, устройства перехвата IMSI применяются на крупных митингах, чтобы правоохранительные органы впоследствии могли выяснить, кто на них присутствовал, особенно если эти люди активно призывали других к ним присоединиться.

Кроме того, подобное устройство позволяет специальным приложениям создавать отчеты о пробках на дорогах. При этом сам номер телефона или IMSI не имеет значения, важно лишь, с какой скоростью ваш сотовый телефон перемещается от одной базовой станции к другой, из одной географической зоны в другую. В зависимости от того, за какой промежуток времени телефон оказывается у следующей базовой станции, соответствующий участок дороги отмечается красным, желтым или зеленым цветом.

Правоохранительные органы создали устройства, которые выдают себя за базовые станции сотовой связи. Они разработаны для перехвата разговоров и текстовых сообщений. В США правоохранительные органы также пользуются устройствами, с помощью которых можно определить IMSI мобильного телефона. Он перехватывается менее чем за секунду и без каких-либо уведомлений.

Ваше мобильное устройство, когда оно включено, находится на связи сразу с несколькими базовыми станциями. При этом обработкой телефонных соединений, текстовых сообщений и интернет-сессий передачи данных занимается ближайшая из них. По мере ваших перемещений телефон подсоединяется к ближайшей базовой станции, и в случае необходимости обработка вызова передается от станции к станции, а вы получаете бесперебойную связь. Остальные ближайшие станции находятся в режиме ожидания, поэтому, если вы перемещаетесь из пункта А в пункт Б и одна из станций может обеспечить более высокий уровень сигнала, смена станции происходит довольно гладко, благодаря чему соединение обычно не прерывается.

Достаточно сказать, что ваше мобильное устройство передает уникальный код, который получает и фиксирует определенное число базовых станций. Поэтому любой, кто просмотрит файлы данных той или иной базовой станции, увидит временный идентификатор мобильной станции (Temporary Mobile Subscriber Identity, TMSI) каждого абонента, оказавшегося в данной зоне в тот или иной момент времени, независимо от того, звонил он кому-нибудь или нет. Правоохранительные органы могут запросить (и запрашивают) у мобильного оператора все эти данные, включая информацию о личности каждого конкретного абонента.

Как правило, если просмотреть файлы данных только с одной базовой станции, можно выяснить лишь, что кто-то проходил мимо и мобильный телефон этого человека передал сигнал данной станции, находясь в режиме ожидания. Если был совершен звонок или пересылались какие-либо

данные, в файлах будет также запись об этом вызове и его длительности.

Однако с помощью файлов данных с нескольких базовых станций можно отследить местонахождение абонента. Большинство мобильных устройств отправляют сигнал сразу трем или более базовым станциям. Опираясь на файлы данных с этих станций и сравнив уровень полученных ими сигналов, можно с довольно высокой степенью точности вычислить (методом триангуляции) местонахождение телефона. Таким образом, телефон, ваш ежедневный спутник — это фактически устройство слежения.

Как можно избежать отслеживания?

Чтобы подключиться к оператору сотовой связи, необходимо заключить договор и указать свое имя, адрес и номер паспорта. Кроме того, если вы покупаете телефон в рассрочку, банк проверит вашу кредитную историю, чтобы убедиться в вашей платежеспособности. Это неизбежно.

Разумная альтернатива — одноразовый телефон. Предоплаченные сотовые телефоны, если их часто менять (например, раз в неделю или раз в месяц), позволяют оставаться инкогнито. Ваш TMSI появится в файлах данных базовых станций, а затем снова исчезнет, и, если вы соблюдали секретность при покупке телефона, по нему невозможно будет отследить личность владельца. Предоплаченные мобильники до сих пор привязаны к учетной записи пользователя, поэтому и IMSI будет приписан к этой же учетной записи. Следовательно, анонимность абонента зависит от того, как человек приобрел этот одноразовый телефон.

Для наглядности представим себе, что при покупке одноразового телефона вам удалось не оставить зацепок, которые могли бы вывести на вас. Вы выполнили все рекомендации из предыдущей главы и попросили не связанного с вами человека купить вам телефон за наличные.

Действительно ли такой телефон нельзя отследить? Если ответить коротко, то нет.

Поучительная история: однажды в 2007 году из порта в Мельбурне пропал контейнер с экстази стоимостью 500 млн долл. Владелец контейнера, Пэт Барбаро, известный наркоторговец, засунул руку в карман, достал один из двенадцати сотовых телефонов и набрал номер местного репортера, Ника Маккензи, который знал его под именем «Стэн». Затем Барбаро отправил Маккензи текстовое сообщение с другого одноразового телефона, пытаясь «анонимно» разузнать о ходе журналистского расследования пропажи контейнера. Как мы увидим, этот номер не прошел.

Одноразовые телефоны, что бы ни думало большинство людей, на самом деле не совсем анонимные. В соответствии с американским законом о содействии провайдеров телекоммуникационных услуг правоохранительным органам (закон CALEA, Communications Assistance for Law Enforcement Act) сведения об идентификаторах IMSI, связанных с одноразовыми телефонами, передаются правоохранительным органам точно так же, как IMSI обычных абонентов. Другими словами, сотрудник правоохранительных органов может идентифицировать одноразовый телефон так же просто, как и обычный мобильный телефон. Конечно, невозможно вычислить владельца такого телефона просто на основании IMSI, но владелец может выдать себя сам.

В Австралии, где закон CALEA не действует, правоохранительным органам удалось отследить множество телефонов Барбаро привычными методами. Например, детективы могли обратить внимание на то, что через несколько секунд после звонка с его личного телефона эта же базовая станция зафиксировала еще один телефонный вызов или текстовое сообщение с некого одноразового телефона. Если по данным базовых станций одни и те же IMSI часто оказываются на одной и той же территории одновременно, это может свидетельствовать о том, что эти телефоны принадлежат одному и тому же человеку.

Проблема Барбаро, у которого в распоряжении было несколько сотовых телефонов, заключалась в том, что, какой бы из них он ни взял, личный или одноразовый, сигнал передавался через одну и ту же базовую станцию. В файлах данных этой станции записи о звонках с одноразовых телефонов отображались рядом с записями о вызовах с его личного телефона. По телефону с SIM-картой, зарегистрированной на имя абонента, органы правопорядка могут легко отследить владельца и установить его личность. На этих фактах можно было построить пригодное для суда дело против Барбаро, особенно если бы аналогичная ситуация повторилась в другом месте. Так австралийские власти сумели предъявить Барбаро обвинение в организации транспортировки одной из крупнейших партий экстази в австралийской истории.

Подводя итог, Маккензи сказал: «С того дня, когда в моем кармане зазвонил сотовый и в мою жизнь ненадолго ворвался “Стэн”, меня особенно стал интересовать вопрос о том, что люди, какие бы меры предосторожности они ни предпринимали, общаясь, оставляют за собой след».

Конечно, можно пользоваться только одноразовым телефоном. В таком случае вам время от времени придется анонимно докупать дополнительное время с помощью карт оплаты или биткойнов. Это можно сделать, подключившись к общедоступной Wi-Fi-сети, изменив MAC-адрес

сетевой карты (см. далее в этой книге) и не попадая в поле зрения камер наблюдения. Или можно, как уже описывалось в предыдущей главе, заплатить незнакомцу, чтобы тот за наличные приобрел вам дополнительное время в каком-нибудь отдаленном магазине. Так будет дороже и, вероятно, возникнут определенные неудобства, но у вас будет анонимный телефон.

Несмотря на кажущуюся новизну, сотовая связь существует уже более сорока лет и, как и проводная телефония, частично опирается на устаревшие технологии, что делает ее уязвимой с точки зрения конфиденциальности.

С каждым следующим поколением сотовая связь приобретала новые возможности, в основном связанные с более эффективной и быстрой передачей данных. Мобильные телефоны первого поколения, или 1G, стали доступны в 1980-х годах. Эти первые Ю-сети и телефонные аппараты использовали аналоговую связь и опирались на несколько разных стандартов. В 1991 году появилась сотовая связь второго поколения (2G). 2G-связь объединяла в себе два стандарта: Global System for Mobile (GSM) и Code Division Multiple Access (CDMA). Также она включала в себя систему обмена короткими текстовыми сообщениями (SMS), сервис USSD и ряд других протоколов быстрого обмена данными, которые существуют и по сей день. Сейчас мы пользуемя 4G/LTE-связью, и скоро появится 5G.

Независимо от того, какое поколение связи (2G, 3G, 4G или 4G/LTE) поддерживает определенный оператор сотовой связи, он в обязательном порядке опирается на международный набор сигнальных протоколов, известный как Система сигнализации, или ОКС (общий канал сигнализации). Система сигнализации (сейчас актуальна 7-я версия), помимо прочего, обеспечивает непрерывность мобильной связи, когда вы едете по трассе и перемещаетесь от одной базовой станции к другой. Она также может быть одним из инструментов слежения. ОКС-7 прекрасно справляется со всеми задачами, связанными с маршрутизацией вызова, в частности:

• Установление нового соединения для вызова.

• Прерывание этого соединения, когда вызов завершен.

• Выставление счета той стороне, которая совершает вызов.

• Управление дополнительными возможностями, такими как переадресация вызова, отображение имени и номера телефона вызывающей стороны, трехсторонняя связь и другие услуги интеллектуальной сети связи.

• Бесплатные вызовы на номера с кодом 800 и 888 и платные на номера 900.

• Услуги беспроводной связи, включая идентификацию пользователя, передачу данных и мобильный роуминг.

Выступая с речью на Всемирном конгрессе хакеров (Chaos Communication Congress), ежегодной хакерской конференции в Берлине, Тобиас Энгель, основатель компании Sternraute, и Карстен Нол, ведущий научный сотрудник организации Security Research Labs, рассказали, что, пользуясь уязвимостью ОКС-7, они могут не только определить местоположение абонента сотовой сети в любой точке мира, но и прослушивать телефонные разговоры. А если не удалось прослушать соединение в режиме реального времени, можно записать разговор и переданные текстовые сообщения в зашифрованном виде, а позже расшифровать их.

Выступая с речью на Всемирном конгрессе хакеров (Chaos Communication Congress), ежегодной хакерской конференции в Берлине, Тобиас Энгель, основатель компании Sternraute, и Карстен Нол, ведущий научный сотрудник организации Security Research Labs, рассказали, что, пользуясь уязвимостью ОКС-7, они могут не только определить местоположение абонента сотовой сети в любой точке мира, но и прослушивать телефонные разговоры.

Вся система защищена ровно настолько, насколько защищено ее самое слабое звено. Энгель и Нол обнаружили, что хотя развитые европейские и североамериканские страны потратили миллиарды долларов на создание относительно защищенных и безопасных 3G и 4G-сетей, они все равно вынуждены пользоваться ОКС-7 (Системой сигнализации № 7) в качестве основного протокола.

ОКС-7 отвечает за установление соединения, биллинг, маршрутизацию вызовов и обмен информацией.

Это означает, что, если вы получили доступ к ОКС-7, вы можете управлять вызовом. ОКС-7 позволяет хакеру через малоизвестного оператора сотовой связи где-нибудь в Нигерии подключаться к вызовам на территории Европы и США. По словам Энгеля, «это все равно что обезопасить главный вход в дом, но оставить черный ход широко открытым».

Энгель и Нол протестировали метод взлома, который заключается в переадресации вызова: хакер с помощью ОКС-7 переадресует вызов на себя, а лишь потом перенаправляет его абоненту-

получателю. Когда хакер организовал процесс, он может прослушивать все телефонные вызовы, совершаемые интересующим его человеком, из любой точки мира.

Другая стратегия взлома выглядит следующим образом: хакер устанавливает радиоантенны и перехватывает все вызовы и текстовые сообщения с мобильных телефонов в данной местности. Столкнувшись с зашифрованными соединениями в SG-сетях, хакеры могут запросить у ОКС-7 необходимый ключ дешифрования.

«Все происходит автоматически, по нажатию кнопки, — сказал Нол. — Я вдруг увидел тут идеальную возможность для шпионажа, можно записывать и расшифровывать практическую любую сеть… Это сработало во всех проверенных нами сетях». Затем он перечислил почти всех крупных операторов сотовой связи в Северной Америке и Европе, в общей сложности около 20 компаний.

Нол и Энгель также обнаружили, что могут определить местоположение любого сотового телефона благодаря такой функции ОКС-7, как Any Time Interrogation (ATI). Вернее, они могли это делать до тех пор, пока в начале 2015 года функция не прекратила свое существование. Однако чтобы предоставлять свои услуги, все операторы должны отслеживать местонахождение абонентов, поэтому у ОКС-7 есть другие функции, позволяющие осуществлять дистанционное наблюдение за пользователями. Необходимо отметить, что операторы сотовой связи по большей части устранили уязвимости, обнародованные Нолом и Энгелем на конференции.

Возможно, вам кажется, что для конфиденциальности разговоров по сотовому телефону достаточно одного шифрования. Начиная с поколения 2G, соединения в GSM-телефонах шифруются. Однако самые первые технологии шифрования соединений в 2G-сетях были ненадежными и не оправдали себя. К сожалению, стоимость перехода с 2G на 3G-связь для многих операторов оказалась непомерно высокой, поэтому устаревшие стандарты 2G были широко распространены вплоть до 2010 года.

Летом 2010 года группа ученых под руководством Нола разделила все возможные ключи шифрования, используемые в 2G-сетях стандарта GSM, и переработала полученные цифры, получив так называемую радужную таблицу — список предварительно подобранных ключей и паролей. Они опубликовали эту таблицу, чтобы операторы сотовой связи по всему миру увидели, насколько уязвимым было шифрование в сетях GSM поколения 2G. Каждый пакет (или блок данных, передаваемых от отправителя получателю) голосовых, текстовых или иных данных, отправляемых по сети 2G GSM, с помощью радужной таблицы теперь можно было расшифровать за несколько минут. Это был жестокий урок, но ученые решили, что он необходим. Когда ранее Нол с коллегами демонстрировали операторам свои открытия, все предостережения проходили мимо ушей. Показав, как можно взломать шифрование в сети 2G GSM, они в той или иной степени подтолкнули операторов к переменам.

Летом 2010 года группа ученых под руководством Нола разделила все возможные ключи шифрования, используемые в 2G-сетях стандарта GSM, и переработала полученные цифры, получив так называемую радужную таблицу — список предварительно подобранных ключей и паролей. Они опубликовали эту таблицу, чтобы операторы сотовой связи по всему миру увидели, насколько уязвимым было шифрование в сетях GSM поколения 2G. Каждый пакет (или блок данных, передаваемых от отправителя получателю) голосовых, текстовых или иных данных, отправляемых по сети 2G GSM, с помощью радужной таблицы теперь можно было расшифровать за несколько минут.

Важно отметить, что 2G-связь до сих пор поддерживается, а операторы подумывают о том, чтобы продать доступ к своим старым 2G-сетям под «Интернет вещей», т. е. так называемые «умные устройства» (подключенные к Интернету устройства, кроме компьютера — например, телевизор или холодильник), которые передают данные лишь время от времени. Если это произойдет, мы должны будем убедиться, что сами эти устройства оснащены функцией сквозного шифрования, поскольку, как нам теперь известно, на шифрование, обеспечиваемое 2G-сетями, полагаться не стоит.

Разумеется, прослушка существовала и до распространения мобильных устройств. Для Аниты Буш кошмар началася утром 20 июня 2002 года, когда ее разбудил нетерпеливый стук в дверь. Стучал сосед, который увидел пулевое отверстие в лобовом стекле ее машины, припаркованной около дома. Но это было не все: на капоте кто-то оставил розу, мертвую рыбу и записку с одним словом «Остановись». Позже Анита выяснила, что ее телефонные разговоры прослушивались, и отнюдь не правоохранительными органами.

История с пулевым отверстием и мертвой рыбой напоминала сцену из дешевого голливудского фильма про гангстеров, и на то были причины. Буш, опытная журналистка, на тот момент всего несколько недель проработала внештатным сотрудником газеты Los Angeles Times и писала о растущем влиянии организованной преступности в Голливуде. Особенно ее интересовали Стивен Сигал и его бывший партнер по бизнесу Джулиус Р. Нассо, которого подозревали в связях с нью-йоркской мафией, пытавшейся вытянуть из Сигала деньги.

После того как Анита нашла на своей машине записку, ей поступило несколько телефонных звонков. Звонивший, по всей вероятности, хотел поделиться какой-то информацией о Сигале. Гораздо позже Буш узнала, что этого человека нанял Энтони Пелликано, некогда очень известный в Лос-Анджелесе частный детектив, которого к тому моменту, когда Буш стала получать угрозы, ФБР подозревало в незаконной прослушке телефонных разговоров, подкупе должностных лиц, хищении персональных данных и вымогательстве. Пелликано прослушивал домашний телефон Буш и выяснил, что она пишет статью о его клиентах. Рыбья тушка на машине была попыткой предостеречь ее.

Обычно, когда говорят о телефонном шпионаже, речь идет о телефонных соединениях, но американское законодательство рассматривает это понятие в более широком смысле, включая сюда также перехват электронных писем и текстовых сообщений. Пока что мы сосредоточим свое внимание на обычных стационарных телефонах.

Они устанавливаются в доме или в офисе и подключаются с помощью кабеля, и для их прослушивания необходимо непосредственно (физически) подключиться к нему. Раньше у всех телефонных компаний были массивы коммутаторов, которые представляли собой своеобразные прослушивающие устройства. Иными словами, в распоряжении телефонной компании находилась специальная аппаратура, с помощью которой к целевому телефонному номеру можно было подключаться прямо из центрального офиса. Существует и дополнительное оборудование, которое отправляет вызов на эту аппаратуру и контролирует состояние целевого номера. В наши дни этот вид прослушки канул в Лету: все телефонные компании обязаны отвечать техническим требованиям CALEA.

Хотя в настоящее время все больше людей переходит на мобильные телефоны, многие по-прежнему не отказались от стационарных аппаратов, просто по привычке.

Другие пользуются так называемой IP-телефонией (VoIP), т. е. телефонной связью через Интернет, которая осуществляется через проводной или беспроводной Интернет, из дома или офиса. Будь то физический коммутатор телефонной компании или виртуальный, у правоохранительных органов есть возможность прослушивать телефонные звонки.

Принятый в 1994 году закон CALEA обязывает производителей телекоммуникационного оборудования и провайдеров телекоммуникационных услуг модифицировать аппаратуру таким образом, чтобы правоохранительные органы могли прослушивать линию. Иными словами, в соответствии с законом CALEA, любой вызов по стационарному телефону в США теоретически может прослушиваться. А в соответствии с новыми поправками к закону CALEA правоохранительным органам для прослушки не всегда требуется получать ордер. Однако обычным людям законодательство по-прежнему запрещает прослушивать чужие телефонные вызовы, поэтому Энтони Пелликано нарушил закон, когда шпионил за Анитой Буш и другими людьми. Среди объектов, за которыми вел слежку Пелликано, оказались даже голливудские звезды, такие как Сильвестр Сталлоне, Дэвид Кэррадайн, Кевин Нилон и прочие.

В этот же список попала также моя подруга Эрин Финн, бывший парень которой был одержим ею и хотел следить за каждым ее шагом. А раз ее телефон прослушивался, я тоже оказывался под прицелом, когда звонил ей. Самая приятная часть этой истории состоит в том, что компания AT&T, проигравшая по коллективному иску, заплатила мне несколько тысяч долларов компенсации за то, что Пелликано прослушивал мои переговоры с Эрин Финн. В этом есть некая ирония, поскольку обычно это я прослушиваю других, а не наоборот. Пелликано, вероятно, преследовал более корыстные цели, чем я: например, он пытался заставить свидетелей не давать показаний на суде или говорить строго определенные вещи.

В середине 1990-х годов для прослушки телефонных переговоров требовалась помощь технических специалистов. Поэтому Пелликано или одному из его людей пришлось бы заплатить кому-то из сотрудников телекоммуникационной компании PacBell, чтобы тот осуществил врезку в линию Буш или Финн. Монтерам удалось установить необходимое для прослушки телефонов оборудование непосредственно в офисе Пелликано в Беверли-Хиллз. В этом случае не проводилось никаких манипуляций с телефонными распределительными коробками или собственно аппаратами по месту проживания объектов прослушки, хотя и это тоже было возможно.

Возможно, вы помните из моей предыдущей книги («Призрак в сети») историю о том, как я однажды отправился из Калабасаса, где жил мой отец, в Лонг-Бич, чтобы установить прослушку на телефонную линию, которой пользовался Кент, друг моего умершего брата. Мой брат погиб от передозировки наркотиков, но в этой истории было много неясного, и создавалось впечатление, будто Кент на самом деле знал больше, чем рассказал мне, хотя позднее я выяснил, что он все-таки был ни при чем. Из подсобного помещения многоквартирного дома, где жил Кент, я позвонил в определенный отдел телефонной компании GTE (General Telephone and Electronics) и представился монтером, чтобы выяснить, где находится кабель, подключенный к телефону Кента. Оказалось, что телефон Кента был подключен к линии, проходившей через совсем другое многоквартирное здание. И уже в том, другом подсобном помещении я смог подсоединить свой управляемый голосом

магнитофон к его телефонной линии, установив его в распределительной коробке (через которую монтер телефонной компании подключает линии к квартирам).

После этого каждый раз, когда Кент кому-нибудь звонил, я мог записывать все, о чем говорили он и его собеседник, а сам Кент об этом даже не знал, хотя следует отметить, что запись производилась в режиме реального времени в отличие от ее прослушивания. Каждый день на протяжении следующих 10 дней я тратил 60 минут на дорогу к дому Кента, слушал записи, пытаясь выяснить, не упоминался ли в разговорах мой брат. К сожалению, там ничего не было. Через несколько лет я узнал, что, по всей вероятности, к смерти брата был причастен мой дядя.

Учитывая, как легко мне и Пелликано удавалось прослушивать личные телефонные звонки, как можно говорить о невидимости, если вы пользуетесь стационарным телефоном, который, кажется, просто создан для слежки? Никак, если не купить специальное оборудование. Для истинных параноиков существуют специализированные стационарные телефоны, которые шифруют всю голосовую коммуникацию по проводной связи. Такие аппараты эффективно решают проблему перехвата личных телефонных разговоров, но лишь в том случае, если применяются обеими сторонами, иначе телефонное соединение без проблем можно прослушать. Остальные могут избежать прослушки благодаря определенным приемам.

Переход к цифровой телефонии привел к тому, что перехватывать телефонные соединения стало проще, а не наоборот. Сейчас, если необходимо установить прослушку на цифровую линию связи, это можно сделать удаленно. Коммутационный компьютер просто создает второй, параллельный поток данных, при этом отсутствует необходимость в дополнительном оборудовании. Кроме того, так гораздо труднее определить, прослушивается ли данная линия. В большинстве случаев такая прослушка обнаруживается лишь по случайному стечению обстоятельств.

Вскоре после летних Олимпийских игр в Греции в 2004 году инженеры компании Vodafone-Panafon устранили вредоносную программу, которая, как выяснилось, функционировала в сотовой сети этого оператора более года. На практике правоохранительные органы перехватывают все передаваемые по любой сотовой сети голосовые и текстовые сообщения с помощью системы дистанционного управления (RES), цифрового эквивалента прослушки по аналоговым каналам. Когда объект под наблюдением звонит по мобильному телефону, RES создает второй поток данных, по которому информация поступает непосредственно сотруднику правоохранительных органов.

Обнаруженная в Греции вредоносная программа внедрилась в систему RES оператора Vodafone, а это значит, что доступ ко всем разговорам в сети Vodafone получил кто-то еще, помимо сотрудников правоохранительных органов. Как выяснилось, злоумышленников интересовали высокопоставленные чиновники. Во время Олимпийских игр некоторые страны, например США и Россия, использовали собственные закрытые системы связи для общения на государственном уровне. Главы других государств и представители деловых кругов со всего мира пользовались взломанной системой компании Vodafone.

Расследование показало, что во время Олимпийских игр в Греции прослушивались телефонные переговоры греческого премьер-министра, его жены, министра национальной безопасности, министра иностранных дел, министра торгового флота и министра юстиции, мэра Афин и греческого комиссара ЕС. Кроме того, прослушивались телефоны, принадлежавшие членам правозащитных организаций, антиглобалистам, членам правящей партии «Новая демократия», генштабу военно-морских сил Греции, а также борцам за мир и греко-американскому персоналу посольства США в Афинах.

Слежка могла продолжаться гораздо дольше, если бы сотрудники оператора Vodafone не обратились к своему поставщику телекоммуникационного оборудования, компании Ericsson, пытаясь разобраться с несколькими не связанными между собой жалобами на участившиеся случаи сбоев в доставке текстовых сообщений. Компания Ericsson провела диагностику и сообщила оператору Vodafone, что было обнаружено вредоносное программное обеспечение.

Прошло уже более десяти лет, а мы, к сожалению, так и не узнали, кто это сделал и зачем. И даже как часто такое случается. Что еще хуже, компания Vodafone явно вела расследование довольно небрежно. К примеру, главные файлы данных, которые могли бы пролить свет на ситуацию, исчезли. А вместо того, чтобы позволить вредоносной программе работать и после обнаружения — так часто поступают во время расследований киберпреступлений, — компания Vodafone резко удалила ее из своей системы, что могло спугнуть злоумышленников, которые сумели быстро замести следы.

Эта история — наглядный пример того, как уязвимы наши мобильные телефоны перед прослушкой. Но, пользуясь цифровым телефоном, вы все же можете стать невидимым.

Помимо сотовых и устаревших стационарных телефонов существует третий вариант телефонной связи (о котором я говорил ранее) — IP-телефония (VoIP). Это отличная возможность для тех беспроводных устройств, на которых производителем не предусмотрена возможность телефонных

переговоров, например Apple iPod Touch. У IP-телефонии больше сходства с интернет-серфингом, чем с вызовом по обычному телефону. Для стационарных телефонов необходим медный кабель. Работа мобильных телефонов осуществляется через базовые станции сотовых сетей. IP-телефония просто передает ваш голос по Интернету — либо с помощью кабеля, либо через беспроводное интернет-соединение. IP-телефония также доступна на мобильных устройствах, таких как ноутбук или планшет, независимо от того, обладает ли устройство поддержкой сотовых сетей.

Из соображений экономии многие люди дома и на работе подключились к системам IP-телефонии, предоставляемым интернет-провайдерами или телефонными компаниями. Для передачи голосового сигнала необходим кабель «витая пара» или «оптоволокно» — тот, с помощью которого транслируется потоковое видео, и широкополосный Интернет.

Хорошая новость заключается в том, что в системах IP-телефонии применяется шифрование, в частности нечто под названием SDES (англ. Session Description Protocol Security Descriptions — дескрипторы безопасности протокола SDP). Плохая новость в том, что сам по себе метод SDES не слишком безопасен.

Отчасти проблема SDES заключается в том, что ключ шифрования не передается по криптографическому протоколу SSL/TLS, обеспечивающему безопасную передачу данных. Если сторона не поддерживает SSL/TLS, то ключ отправляется в открытом виде. Вместо асимметричного шифрования используется симметричное шифрование, из чего следует, что генерируемый отправителем ключ необходимо каким-то образом сообщить получателю, чтобы тот мог дешифровать телефонное соединение.

Допустим, Боб хочет позвонить Элис, которая находится в Китае. IP-телефон Боба использует метод SDES для шифрования вызовов и сгенерировал новый ключ. Бобу нужно каким-то образом передать этот новый ключ Элис, чтобы ее устройство могло дешифровать телефонный вызов и разговор состоялся. SDES предлагает следующее решение: отправить ключ провайдеру Боба, который затем передаст его провайдеру Элис, который в свою очередь сообщит его самой Элис.

Вы видите слабое место? Помните, что говорилось о сквозном шифровании в предыдущей главе? Информация защищена до тех пор, пока получатель не примет ее со своей стороны. Но метод SDES предполагает, что ключ станет известен провайдеру Боба и, если его провайдер отличается от провайдера Элис, вызов будет зашифрован от провайдера Элис самой Элис. О значении этого разрыва можно спорить. Нечто подобное происходит и при общении через Skype или Google Voice. Новые ключи генерируются для каждого нового соединения, но эти ключи передаются в Microsoft и Google соответственно. Не слишком внушает доверие, если вам важно, чтобы беседа была приватной.

К счастью, существует возможность сквозного шифрования при пользовании IP-телефонией с мобильного телефона.

Компания Open Whisper Systems разработала приложение Signal, которое представляет собой бесплатную открытую систему IP-телефонии для мобильных телефонов. С его помощью пользователи Android и iOS получают возможность по-настоящему эффективно защитить телефонные переговоры с помощью сквозного шифрования.

Главное преимущество приложения Signal — то, что ключами распоряжаются только тот, кто совершает вызов, и тот, кто его принимает, без участия каких-либо посредников. Иными словами, как и в ситуации с SDES, новые ключи генерируются для каждого вызова, но ключи существуют в единственном экземпляре и хранятся только на устройствах пользователей. Закон CALEA предоставляет правоохранительным органам доступ к информации по каждому конкретному соединению, но в этом случае они увидят лишь зашифрованный трафик, что совершенно неинформативно. А у разработчика приложения Signal, некоммерческой организации Open Whisper Systems, нет этих ключей, так что приходить к ним с судебным ордером бессмысленно. Ключи хранятся только на устройствах абонентов (совершающего вызов и принимающего его). По завершении соединения эти ключи уничтожаются.

В настоящий момент закон CALEA не распространяется на конечных пользователей или на их устройства.

Возможно, вы думаете, что из-за шифрования ваш сотовый телефон будет быстрее разряжаться. Будет, но ненамного. Приложение Signal отправляет пользователям push-уведомления, подобно WhatsApp или Telegram. Поэтому вас будут оповещать только о поступающих вызовах, что сводит к минимуму расход батареи. Также приложения для Android и iOS задействуют аудиокодеки и алгоритмы управления буфером, свойственные сотовой сети, поэтому опять же шифрование не будет сильно разряжать батарею во время разговора.

Помимо сквозного шифрования, в приложении Signal также реализовано свойство PFS (англ. Perfect Forward Secrecy — совершенная прямая секретность). Что это такое? Это свойство, благодаря

которому ключ шифрования для каждого следующего вызова будет слегка отличаться от предыдущего, и если кто-то сумеет получить доступ к вашему конкретному зашифрованному телефонному соединению и ключу шифрования, он не сможет прослушивать все остальные соединения. Основой всех ключей остается исходный ключ, но если кто-то завладеет одним из ключей, это вовсе не значит, что потенциальный злоумышленник сможет прослушивать все ваши дальнейшие переговоры.

Глава 4

ЗАШИФРОВАН — ЗНАЧИТ ВООРУЖЕН!

Если бы кто-нибудь прямо сейчас взял ваш незаблокированный смартфон, он получил бы доступ ко всей вашей электронной переписке, к вашему аккаунту в социальной сети Facebook и, вероятно, даже к вашему личному кабинету на сайте Amazon. На смартфонах теперь не нужно вводить логин и пароль для каждого отдельного сервиса, как при работе на ноутбуке или настольном компьютере. Мы пользуемся мобильными приложениями, которые запоминают данные учетной записи, достаточно авторизоваться в них единожды. Помимо фотографий и музыки, смартфоны предлагают еще одну уникальную возможность — обмен текстовыми SMS-сообщениями. Если на вашем сотовом телефоне нет защиты и он попадет в чужие руки, то завладевший им человек получит доступ в том числе и к вашим SMS-сообщениям.

Рассмотрим следующую историю. В 2009 году житель города Лонгвью (штат Вашингтон) Дэниел Ли был арестован по подозрению в продаже наркотиков. Пока он находился под стражей, полиция просмотрела данные на его сотовом телефоне (который не был защищен паролем) и сразу же нашла несколько текстовых сообщений о наркотиках. Одно из них было получено от человека под ником «Z-Jon».

Текст был следующим: «У меня на руках сто тридцать за одну шестидесятую, которую ты дал мне вчера вечером». Согласно протоколу судебного заседания, полиция города Лонгвью не просто читала сообщения от Z-Jon, но и активно на них отвечала, чтобы организовать собственную сделку. Полицейские отправили человеку, записанному как Z-Jon, сообщение от имени Дэниела Ли, спросив: «Нужно ли ему еще?» Контакт Z-Jon ответил: «Да, было бы круто». Когда Z-Jon (настоящее имя которого Джонатан Роден) пришел на встречу, полиция города Лонгвью арестовала его за попытку купить героин.

Также в телефоне Ли внимание полицейских привлекла еще одна переписка, и они аналогичным образом арестовали Шона Дэниела Хинтона.

Оба арестованных подали апелляцию, и при содействии Американского союза защиты гражданских свобод им удалось добиться того, что Верховный суд штата Вашингтон в 2014 году отменил приговоры, вынесенные Родену и Хинтону судом более низкой инстанции. Основанием для отмены вердикта стало проявленное со стороны полиции злоупотребление уверенностью подсудимых в конфиденциальности переписки.

Судьи пояснили, что, если бы Ли первым прочитал сообщения от Родена и Хинтона или поручил полицейским ответить на них фразой: «Дэниела здесь нет», в обоих случаях ситуация была бы принципиально иной. «Текстовые сообщения можно рассматривать как часть того личного пространства, куда также входят телефонные разговоры, запечатанные письма и прочие традиционные формы общения, которые исторически строго защищаются законами штата Вашингтон», — написал судья Стивен Гонсалес в комментариях к делу Хинтона.

Судьи постановили, что право на конфиденциальность должно распространяться не только на бумажную переписку, но и на цифровую сферу. В США органам правопорядка запрещено вскрывать запечатанные письма без разрешения адресата. Ожидание конфиденциальности является юридическим критерием. Этот критерий необходим, когда речь идет о соблюдении права на конфиденциальность, гарантированного четвертой поправкой к Конституции США. Время покажет, какие судебные решения будут приниматься в дальнейшем и будет ли применяться данный юридический критерий в будущем.

Технология обмена текстовыми сообщениями, известная как SMS (сокр. от англ. Short Message Service), появилась в 1992 году. Сотовые телефоны, даже самые простые (т. е. не смартфоны), позволяют отправлять короткие текстовые сообщения. Текстовые сообщения необязательно передаются по схеме «точка — точка», иными словами, нельзя сказать, что сообщение непосредственно перемещается с одного мобильного телефона на другой. Как и электронные письма, сообщения, которые вы набираете на телефоне, в незашифрованном виде отправляются в SMS-центр (SMSC), элемент сотовой сети, предназначенный для хранения, пересылки и доставки SMS-сообщений — иногда с задержкой в несколько часов.

Исходное текстовое сообщение (отправленное с мобильного телефона, а не через приложение) проходит через SMS-центр оператора сотовой связи, где оно может храниться, а может и нет. Операторы утверждают, что срок хранения сообщений не превышает нескольких дней. По истечении этого срока текстовые сообщения сохраняются только в мобильных телефонах отправителя и получателя, а количество сообщений зависит от модели телефона. Несмотря на эти заверения, я думаю, что все операторы сотовой связи в США хранят текстовые сообщения гораздо дольше, чем утверждают.

Слова операторов вызывают сомнения. Раскрытые Эдвардом Сноуденом документы свидетельствуют о тесном сотрудничестве Агентства национальной безопасности США и как минимум одного оператора, AT&T. По утверждению интернет-издания Wired, начиная с 2002 года, практически сразу после событий 11 сентября Агентство национальной безопасности совместно с AT&T стало создавать секретные помещения на базе некоторых принадлежащих оператору объектов. Одно помещение располагалось в Бриджтоне, штат Миссури, а другое — на улице Фолсом-стрит в центре Сан-Франциско. Позже подобные помещения появились и в других городах, в том числе в Сиэтле, Сан-Хосе, Лос-Анджелесе и Сан-Диего. Их предназначением было пропускать весь телефонный и интернет-трафик, а также электронные письма сквозь специальный фильтр, настроенный на поиск ключевых слов. До сих пор неизвестно, применялся ли этот фильтр к текстовым сообщениям, но есть все основания это предположить. Также мы не знаем, занимается ли чем-то подобным AT&T или какой-либо другой оператор теперь, после разоблачений Сноудена.

Один факт указывает на то, что подобная практика больше не в ходу.

В 2015 году в серии матчей плей-офф, предшествующих Супербоулу 2014 года, команда New England Patriots обыграла Indianapolis Colts со счетом 45:7. Однако победа Patriots не была однозначной. Основанием для споров было то, что команда намеренно использовала слабо накачанные мячи. Национальная футбольная лига (НФЛ) предъявляет жесткие требования к мячу и степени его накачки, и после игры плей-офф выяснилось, что мячи команды New England Patriots не соответствовали этим требованиям. Ключевым звеном расследования были текстовые сообщения, отправленные Томом Брэди, звездным квотербеком Patriots.

Брэди отрицал свою причастность к скандалу. Чтобы доказать свою правоту, ему, скорее всего, нужно было лишь показать следователям все сообщения, написанные им до и во время игры. К сожалению, прямо в день беседы со следователями Брэди внезапно поменял сотовый телефон, которым пользовался с ноября 2014 по 6 марта 2015 года, на новый. Позже он объяснил комиссии, что его старый телефон разбился, а вместе с ним пропали и все сохраненные данные, включая текстовые сообщения. В результате НФЛ дисквалифицировала Брэди на четыре игры, однако позже это решение было отменено в судебном порядке.

«За четыре месяца пользования этим сотовым телефоном Брэди отправил и получил около 10 000 текстовых сообщений, ни одно из которых теперь невозможно прочитать, — сказали представители Лиги. — На слушании дела по апелляции представители мистера Брэди предоставили письмо от оператора сотовой связи, которое подтверждало, что текстовые сообщения, отправленные или полученные с уничтоженного мобильного телефона, не подлежат восстановлению».

Следовательно, раз Том Брэди получил от своего оператора письмо, в котором сообщалось, что его текстовые сообщения исчезли безвозвратно, а сами операторы сотовой связи утверждают, что не хранят их, единственный способ продлить срок существования сообщений — создать резервную копию данных с мобильного телефона и сохранить ее в «облаке». Если облачный сервис, которым вы пользуетесь, предоставлен оператором сотовой связи или же компанией Google или Apple, то у этих компаний может быть доступ к вашим сообщениям. Очевидно, Том Брэди не успел сохранить в «облаке» резервную копию содержимого своего старого телефона перед его внезапной кончиной.

Конгресс не сумел разобраться с проблемой хранения данных в целом и информации с мобильных телефонов в частности. В последнее время в Конгрессе регулярно звучат предложения обязать каждого оператора сотовой связи хранить текстовые сообщения в течение двух лет. В 2015 году Австралия решилась на этот шаг, так что посмотрим, каковы будут последствия.

Так как же сохранить конфиденциальность текстовых сообщений? Во-первых, не пользуйтесь сервисом обмена сообщениями, предоставляемым вашим оператором сотовой связи. Лучше выбрать приложение от стороннего разработчика. Но какое именно?

Чтобы скрыть свою личность онлайн — и сохранить анонимность в Интернете, — необходимо использовать надежное программное обеспечение и программные службы. Эту надежность трудно проверить. Как правило, выпускаемое некоммерческими организациями бесплатное программное обеспечение с открытым кодом оказывается наиболее надежным, поскольку в его разработку вносят свой вклад тысячи людей, замечая каждую деталь, которая кажется подозрительной или уязвимой. При использовании проприетарного программного обеспечения вам, так или иначе, приходится верить производителю на слово.

Обзоры программных инструментов не слишком информативны по своей природе. Из них можно узнать, например, как действуют элементы интерфейса. Автор обзора изучает программу всего несколько дней, а затем делится своими впечатлениями. Он не пользуется ей в обычной жизни, поэтому не может рассказать, что произойдет в дальнейшем. Вы узнаете только о его первом впечатлении.

Кроме того, авторы обзоров не скажут, можно ли доверять той или иной программе. Они вообще не оценивают такие аспекты, как безопасность и конфиденциальность. И тот факт, что данный продукт

выпущен известным разработчиком, вовсе не означает, что он безопасен. По сути, необходимо с особой осторожностью относиться к известным названиям, поскольку они часто внушают нам неоправданное чувство безопасности. Не следует слепо доверять производителям.

В 1990-х годах, когда мне нужно было зашифровать жесткий диск своего компьютера, работавшего под управлением операционной системы Windows 95, я выбрал на сегодняшний день уже давно неактуальную утилиту Norton Diskreet компании Symantec. Питер Нортон был гением. Его первая служебная программа автоматизировала процесс восстановления удаленных файлов на компьютере. Он создал еще множество отличных утилит. Все это происходило в 1980-х, когда лишь немногие умели работать с командной строкой. Но затем он продал свою фирму компании Symantec, и под его именем писать программы стал кто-то другой.

Когда я решил применить инструмент Diskreet, который в настоящее время уже недоступен, алгоритм шифрования DES (англ. Data Encryption Standard — стандарт шифрования данных) с 56-битным ключом считался серьезной защитой. Это было самое надежное шифрование на тот момент. Для сравнения, сейчас мы пользуемся алгоритмом шифрования AES (англ. advanced encryption standard — улучшенный стандарт шифрования) с длиной ключа 256 бит. При шифровании с каждым битом экспоненциально увеличивается количество ключей шифрования, а следовательно, возрастает степень защиты. Стандарт DES-56 считался невероятно надежным ровно до тех пор, пока в 1998 году его не взломали.

Как бы там ни было, я хотел посмотреть, справится ли Diskreet с шифрованием моих данных и поможет ли это скрыть информацию от ФБР, если агенты когда-нибудь доберутся до моего компьютера. После покупки программы я взломал сайт Symantec и нашел исходный код утилиты. Затем я проанализировал, что программа сделала и как она это сделала. Я понял, что Diskreet шифрует данные при помощи ключа в 30 бит, остальные были просто битами заполнения. Это даже менее надежно, чем ключ длиной 40 бит — максимальная разрешенная длина ключа для средств шифрования, экспортируемых из США.

На практике это означало следующее: кто угодно — АНБ, правоохранительные органы или злоумышленник с очень мощным компьютером — мог взломать зашифрованные с помощью программы Diskreet данные, причем сделать это гораздо проще, чем было заявлено, поскольку длина ключа на самом деле составляла далеко не 56 бит. И все же компания заявляла, что утилита использует 56-битный ключ шифрования. Я решил поискать что-нибудь другое.

Откуда обо всем этом мог бы узнать человек, несведущий в этих вопросах? Ниоткуда.

По данным исследовательской компании Niche, несмотря на то что среди молодежи особой популярностью пользуются приложения для социальных сетей (в частности Facebook, Snapchat и Instagram), в целом первую строчку в рейтинге занимают приложения для обмена текстовыми сообщениями (мессенджеры). Недавно проведенное исследование показало, что 87 процентов тинейджеров ежедневно пишут текстовые сообщения, в то время как следующим по популярности приложением (Facebook) ежедневно пользуется 61 процент. По данным исследования, девушки отправляют в среднем по 3952 сообщения в месяц, юноши — около 2815.

Хорошая новость заключается в том, что в наше время популярные мессенджеры шифруют передаваемые сообщения. Плохая новость в том, что не каждый вид применяемого шифрования достаточно надежен. В 2014 году Пол Джерегуи (Paul Jauregui) из компании Praetorian, занимающейся информационной безопасностью, выяснил, что шифрование в WhatsApp уязвимо к атаке, известной как «человек посередине» (Man-in-the-Middle, MitM), когда злоумышленник перехватывает и читает все сообщения, отправляемые жертвой. «Именно такие вещи любит АНБ», — сказал Джерегуи. На момент написания данной книги ситуация изменилась — теперь на устройствах Android и iOS приложение применяет сквозное шифрование. Кроме того, компания Facebook, которой принадлежит WhatsApp, стала использовать шифрование в своем приложении Facebook Messenger, количество пользователей которого насчитывает 900 миллионов человек. Это необязательная опция — чтобы воспользоваться ей, надо специально включить режим «Секретная переписка».

Неприятный момент связан с архивируемыми данными. Большинство мобильных приложений для обмена текстовыми сообщениями не шифруют заархивированные данные, независимо от того, где именно они хранятся — на вашем устойстве или на сервере. Такие приложения, как AOL Instant Messenger, Blackberry Messenger и Skype, хранят текстовые сообщения в незашифрованном виде. Это означает, что провайдер услуг может прочитать эти сообщения (если они хранятся в облаке) и, исходя из их содержания, настроить рекламу. Также это означает, что правоохранительные органы — или, наоборот, злоумышленники, — заполучив ваше устройство, также смогут прочитать все сообщения.

Другой спорный вопрос — это хранение данных, о котором мы уже говорили ранее: как долго неактивные данные остаются неактивными? Если вышеупомянутые приложения архивируют сообщения в незашифрованном виде, сколько времени они их хранят? Корпорация Microsoft,

которой принадлежит Skype, заявила, что «некоторые из наших продуктов для обмена сообщениями и синхронизации файлов, такие как Outlook и OneDrive, систематически сканируют содержимое для автоматического обнаружения подозрительных несанкционированных рассылок (спама), вирусов, оскорбительных действий или URL-адресов, помеченных как мошеннические, фишинговые или как ссылки на вредоносные программы». Напоминает автоматическую антивирусную проверку в электронной почте. Однако далее идет такой текст: «Наконец мы будем получать доступ, передавать, раскрывать или хранить ваши персональные данные, включая ваше личное содержимое (например, содержимое электронной почты на странице Outlook.com или файлы, которые находятся в личных папках в службе OneDrive), в целях осуществления действий, необходимых для: (1) соблюдения действующего законодательства или предоставления ответов на запросы в рамках судебного процесса, в том числе от правоохранительных органов или иных государственных организаций…»

Звучит как-то не очень. Сколько хранятся такие данные?

Вероятно, практически для каждого из нас первым мессенджером стал AOL Instant Message (AIM). Он был актуален долгое время. Разработанное для обычных настольных компьютеров приложение AIM изначально представляло собой маленькое диалоговое окно, которое появлялось в нижнем правом углу экрана. В наше время этот мессенджер можно установить и на мобильное устройство. Но, что касается конфиденциальности, тут есть свои подводные камни. Во-первых, AIM хранит в архивированном виде все сообщения, когда-либо отправленные через него. И, как и Skype, мессенджер сканирует содержимое этих сообщений. Кроме того, беспокойство вызывает тот факт, что компания AOL хранит сообщения в облаке на случай, если вы когда-либо захотите просмотреть историю переписки с устройства, отличного от того, на котором вы авторизовались в предыдущий раз.

Поскольку данные из AIM не шифруются и благодаря облачному хранилищу их можно просмотреть на любом устройстве, правоохранительные органы и злоумышленники без труда могут получить к ним доступ. Например, мою учетную запись AOL взломал скрипт-кидди, называвший себя в Интернете ником «Virus» — в реальной жизни его зовут Майкл Нивз. Он, применив методы социальной инженерии (иными словами, набрав телефонный номер и мило пообщавшись), сумел выяснить у сотрудников AOL, как ему получить доступ к их внутренней базе данных под названием Merlin. В результате он сумел сменить мой электронный адрес на какой-то другой. После этого ему удалось сбросить мой пароль и прочитать все мои последние сообщения. В 2007 году Нивзу было предъявлено обвинение в четырех тяжких уголовных преступлениях и одном проступке, связанных со взломом «внутренних компьютерных сетей и баз данных компании AOL, включая платежные данные, адреса и данные банковских карт пользователей».

Как справедливо заметили в Фонде электронных рубежей (англ. Electronic Frontier Foundation, EFF), «отсутствие журнальных файлов (логов) — хороший лог». AOL хранит логи.

Разработчики сторонних приложений для обмена текстовыми сообщениями могут заявить, что используют шифрование, но это шифрование может быть недостаточно надежным. На что следует обратить внимание? Если в приложении для обмена текстовыми сообщениями применяется сквозное шифрование, значит, что у третьих лиц нет ключа и он хранится только на устройствах. Также обратите внимание, что если одно из устройств заражено вредоносной программой, то любое шифрование бесполезно.

Существует три основные разновидности приложений для обмена сообщениями.

• Без шифрования — т. е. кто угодно может прочитать ваши сообщения.

• С шифрованием, но не сквозным — т. е. переписку может прочитать третье лицо, например интернет-провайдер, поскольку ему известен ключ.

• Со сквозным шифрованием — т. е. третьи лица не смогут прочитать сообщения, поскольку ключи хранятся только на устройствах конечных пользователей.

К сожалению, большинство общеизвестных мессенджеров, таких как AIM, не обеспечивают должный уровень конфиденциальности. Это касается даже приложений Whisper и Secret. Количество пользователей Whisper исчисляется миллионами, и оно позиционируется как анонимное, однако специалисты обнаружили нестыковки. Whisper отслеживает перемещение своих пользователей, а Secret иногда раскрывает личность пользователя.

Еще одно приложение для обмена сообщениями — это Telegram, в нем используется шифрование, и его считают отличной альтернативой WhatsApp. Он работает на устройствах с Android, iOS и Windows. Однако специалисты выяснили, что серверы Telegram можно скомпрометировать и получить доступ к критическим данным. Кроме того, им удалось без труда извлечь зашифрованные приложением Telegram сообщения даже после их удаления с устройства.

Итак, теперь, когда мы отсеяли несколько популярных вариантов, что остается?

Много чего. Когда вы откроете App Store или Google Play, ищите приложения с поддержкой технологии под названием Off the Record (OTR). Это надежный протокол сквозного шифрования текстовых сообщений, который применяется в некоторых приложениях.

Идеальное приложение для обмена текстовыми сообщениями также должно включать в себя технологию Perfect Forward Secrecy (PFS). Напомню, что это означает генерирование произвольного сессионного ключа, который гарантирует надежность системы. Даже если один из ключей скомпрометирован, с его помощью невозможно прочитать сообщения в будущих сессиях.

Существует несколько приложений с поддержкой как OTR, так и PFS.

Одно из них называется ChatSecure, оно совместимо с операционной системой Android и iOS. Также в этом приложении реализована технология, известная как закрепление сертификата. Это означает, что приложение применяет цифровой сертификат, который удостоверяет личность пользователя и хранится на устройстве. При каждом контакте с серверами ChatSecure сертификат в приложении на вашем устройстве сравнивается с сертификатом в базе. Если сертификаты не совпадают, сессия прерывается. Еще один приятный момент — приложение ChatSecure также шифрует логи, которые хранятся на устройстве, т. е. неактивные данные.

Пожалуй, лучшее из подобных приложений с открытым кодом — это Signal компании Open Whisper Systems. Это приложение работает в операционных системах iOS и Android. (см. **signal.org/ru/**)

Следующее заслуживающее вашего внимания приложение для обмена сообщениями — это CryptoCat. Оно доступно для iPhone и компьютеров под управлением операционной системы Windows, macOS и Linux. Однако у него нет версии для Android.

И на момент написания данной книги разработчики Tor Project, которые ранее создали Tor Browser, как раз выпустили приложение Tor Messenger. Как и браузер, мессенджер применяет сквозное шифрование и скрывает реальный IP-адрес, чтобы сообщения невозможно было отследить. (Однако обратите внимание, что, как и при работе с Tor Browser, выходные узлы могут быть скомпрометированы.) И, как и со всем программным обеспечением Tor, новичку довольно трудно разобраться с этим приложением, но, потратив время и приложив усилия, вы получите полную анонимность переписки.

Также существуют и коммерческие приложения со сквозным шифрованием. Однако тут необходимо оговорить, что это программное обеспечение проприетарно и без независимой экспертизы нельзя быть уверенным в его надежности и безопасности. Одно из таких приложений, Silent Phone, применяет сквозное шифрование. Хотя Silent Phone все-таки хранит часть информации в логах, это делается только в целях совершенствования работы. Ключи шифрования хранятся на устройстве. Это означает, что правительство и правоохранительные органы не смогут вынудить компанию Silent Circle выдать ключи им.

Итак, мы обсудили шифрование данных при передаче и при хранении, а также поговорили о сквозном шифровании, технологиях PFS и OTR. А что же насчет других сервисов, а не приложений, например веб-почты? Что же насчет паролей?

Глава 5

ВОТ МЕНЯ ВИДНО, А ВОТ — УЖЕ НЕТ

В апреле 2013 года Хайрулложон Матанов, 24-летний бывший таксист из Куинси, штат Массачусетс, вместе с двумя друзьями (которые приходились друг другу братьями) отправился в закусочную. Помимо прочего, трое мужчин обсуждали происшествие на Бостонском марафоне: в тот день кто-то недалеко от финиша разместил несколько рисоварок, начиненных гвоздями и порохом, а также установил таймер. Прогремевший взрыв унес жизни трех человек, более двухсот человек получили ранения. Братьями, с которыми Матанов сидел за столом, были Тамерлан и Джохар Царнаевы, которые позже стали главными подозреваемыми в организации теракта.

Хотя Матанов позже заявлял, что ничего не знал о бомбе, он быстро ушел со встречи с представителями правоохранительных органов и немедленно удалил историю посещений в браузере на своем компьютере. Этот незначительный поступок — удаление истории посещений в браузере — стал основанием для обвинений, выдвинутых против него.

Удаление истории посещений в браузере было также одним из пунктов обвинения в деле Дэвида Кернелла, студента, взломавшего электронную почту Сары Пэйлин. Примечательно в этой истории то, что в момент, когда Кернелл очистил историю посещений в браузере, запустил программу дефрагментации диска и удалил скачанные фотографии Пэйлин, он еще не находился под следствием. Получается, что в США нельзя ничего удалять со своего компьютера. Следствие хочет видеть всю историю посещений в браузере.

Юридической основой обвинения против Матанова и Кернелла был закон пятнадцатилетней давности «О реформе учета и отчетности в открытых компаниях и защите интересов инвестора» (как он известен в Сенате) и «Об отчетности, ответственности и прозрачности деятельности корпораций и аудиторов» (как он известен в Палате представителей), который более известен как закон Сарбейнса-Оксли 2002 года (англ. Sarbanes-Oxley Act). Закон был разработан в ответ на служебные преступления руководства корпорации Enron, энергетической компании, которая, как позже выяснилось, обманывала инвесторов и правительство США. Сотрудники правоохранительных органов, занимавшиеся расследованием дела Enron, обнаружили, что множество данных было удалено еще на начальных этапах расследования, поэтому им была доступна лишь частичная информация о делах компании. В результате сенатор Пол Сарбейнс (демократическая партия, штат Мэриленд) и Майкл Оксли (республиканская партия, штат Огайо) внесли в закон ряд пунктов, требующих сохранения вещественных доказательств. Один из них расценивает очистку истории браузера как преступление, если человек оказывается под следствием.

Согласно обвинительному акту большого жюри, Матанов выборочно очистил историю посещений в браузере Google Chrome, удалив данные за несколько дней до той недели, когда произошел теракт (15 апреля 2013). Официально его признали виновным по двум пунктам обвинения: 1) уничтожение, изменение и фальсификация записей, документов и материальных объектов в ходе федерального расследования; и 2) дача заведомо ложных показаний в федеральном расследовании международной и внутренней террористической деятельности. Его приговорили к тридцати месяцам тюрьмы.

До этих пор положение об очистке истории посещений в браузере закона Сарбейнса-Оксли применялось нечасто — в основном в отношении компаний или частных лиц. И да, дело Матанова незаурядное, это резонансное преступление, касающееся государственной безопасности. Однако в последнее время обвинители стали чаще инкриминировать эту статью, разглядев весь ее потенциал.

Если вы не можете помешать третьим лицам просматривать вашу электронную почту, прослушивать телефонные переговоры и читать сообщения, да еще и по закону не можете очистить историю посещений в браузере, что вам остается? Для начала можно попытаться предотвратить сохранение истории.

Во всех браузерах, таких как Firefox (Mozilla), Chrome (Google), Safari (Apple), Internet Explorer и Edge (Microsoft), предусмотрен режим инкогнито, работающий на любом устройстве, будь то компьютер или телефон. Вы открываете новое окно браузера в этом режиме, и он не станет сохранять историю поиска или список посещенных страниц за эту сессию. Как только вы закроете это окно, все следы просмотренных сайтов исчезнут с компьютера или мобильного устройства. За конфиденциальность приходится расплачиваться некоторыми неудобствами: если при работе в приватном режиме вы забудете добавить в закладки интересующий вас сайт, в следующий раз вам придется искать его заново, потому что история не сохраняется (по крайней мере, на вашем устройстве).

Может быть, воспользовавшись таким режимом в Firefox или Chrome, вы почувствуете себя неуязвимым, но, как мы наблюдали на примере электронных писем и текстовых сообщений, ваши

анонимные запросы страницы того или иного сайта все равно проходят через вашего интернет-провайдера или оператора сотовой связи. И ваш провайдер сможет перехватить любую информацию, которая пересылается в незашифрованном виде. Если вы заходите на сайт, который использует шифрование, тогда ваш провайдер получит метаданные, из которых можно узнать, что вы посетили такой-то сайт такого-то числа в такое-то время.

Когда веб-браузер — будь то компьютер или мобильное устройство — устанавливает соединение с веб-сайтом, сначала он выясняет, будет ли использоваться шифрование и, если да, какое именно. Протокол передачи данных называется HTTP. Протокол указывается перед адресом, т. е. типичный URL-адрес может выглядеть следующим образом: . В большинстве случаев можно даже обойтись без «www».

Когда вы подключаетесь к сайту по зашифрованному соединению, протокол меняется. Вместо HTTP вы увидите HTTPS. Теперь URL-адрес выглядит как . HTTPS-соединение безопаснее — в первую очередь потому, что оно происходит по схеме «точка — точка», иначе говоря, вы подключаетесь к сайту напрямую. Также существует множество сетей доставки и дистрибуции контента (англ. Content Delivery Networks, CDN), которые кэшируют страницы, чтобы сократить время их загрузки, независимо от того, в какой точке мира вы находитесь. Поэтому между вами и сайтом есть еще один посредник.

Кроме того, нельзя забывать, что, если вы авторизовались в своем аккаунте Google, Yahoo! или Microsoft, весь сетевой трафик на вашем компьютере или мобильном устройстве будет фиксироваться непосредственно самим аккаунтом — на словах, это делается, чтобы составить ваш поведенческий профиль для настройки рекламных объявлений. Один из способов этого избежать — всегда по завершении работы выходить из своей учетной записи Google, Yahoo! и Microsoft. При необходимости вы можете в любой момент снова авторизоваться.

Кроме того, в мобильные устройства некоторые браузеры встраиваются по умолчанию. Это плохие браузеры. Это мусор, потому что они представляют собой мини-версии браузеров для настольных ПК и ноутбуков, и в них отсутствует ряд функций, отвечающих за безопасность и конфиденциальность, которыми оснащены более надежные версии. Например, на iPhone по умолчанию установлен браузер Safari, но лучше перейти в магазин App Store и скачать мобильную версию браузера Chrome или Firefox. На устройствах под управлением операционной системы Android последних моделей по умолчанию установлен браузер Chrome. Все мобильные браузеры как минимум поддерживают приватный режим.

Если вы пользуетесь планшетом Kindle Fire, то установить Firefox или Chrome будет не так легко, потому что их нет в магазине Amazon. Вам придется пойти обходным путем и установить Firefox или Chrome через браузер Amazon Silk. Чтобы установить мобильную версию программы Firefox на планшет Kindle Fire, необходимо выполнить следующие действия: откройте браузер Silk и перейдите на FTP-сервер Mozilla, затем нажмите кнопку **Go** (Перейти). Выберите файл с расширением .apk.

В режиме инкогнито не создаются временные файлы, поэтому ни в ноутбуке, ни в смартфоне не будет информации о вашей активности в Интернете. Может ли кто-то посторонний посмотреть, что вы делали на том или ином сайте? Да, если взаимодействие с сайтом не было зашифрованным. Здесь необходимо пояснить, что Фонд электронных рубежей (англ. Electronic Frontier Foundation, EFF) создал расширение для браузеров под названием HTTPS Everywhere. Это расширение подходит для настольных версий браузеров Firefox и Chrome и даже для браузера Firefox для Android. В настоящий момент отсутствует версия для iOS. Расширение HTTPS Everywhere приносит ощутимую пользу: первые несколько секунд соединения браузер и сайт обмениваются информацией о том, какой вид защиты будет применяться. Идеальным вариантом будет Perfect Forward Secrecy (PFS), мы уже говорили об этом свойстве в предыдущей главе. Однако не все сайты поддерживают PFS. И согласование вида защиты не всегда завершается выбором PFS — даже когда есть такая возможность. Расширение HTTPS Everywhere способно заставить сайт использовать HTTPS всегда, когда только возможно, даже если нет поддержки PFS.

Поговорим еще об одном факторе, влияющем на безопасность соединения: у каждого веб-сайта должен быть сертификат — независимая гарантия того, что, устанавливая соединение с сайтом, к примеру компании Bank of America, вы действительно будете обмениваться данными с сайтом Bank of America, а не с мошеннической страницей, имитирующей его. Современные браузеры сотрудничают со сторонними организациями, известными как удостоверяющие центры, которые составляют актуальные списки. Каждый раз при соединении с сайтом, который не получил доверенный сертификат, браузер будет выдавать ошибку с предупреждением, что продолжать работу с сайтом вы можете на свой страх и риск. Если вы доверяете содержимому сайта, то можете сделать исключение. В общем, если вы не знакомы с конкретным сайтом, не делайте исключений.

Кроме того, в Интернете используется не один тип сертификатов, а несколько. Самый известный из них, который вы встречаете практически повсеместно, подтверждает только то, что доменное имя принадлежит тому, кто запросил сертификат, пройдя верификацию по электронной почте. Это

может быть кто угодно, но это совершенно неважно — у сайта есть сертификат, знакомый вашему браузеру. То же самое можно сказать и про второй вид сертификатов — подтверждающих подлинность организации в целом. Это означает, что у всех сайтов на данном домене один сертификат с остальными — т. е. у всех поддоменов на сайте mitnicksecurity.com будет один и тот же сертификат.

Однако лучшими считаются сертификаты с расширенной проверкой. Все браузеры при входе на сайт с таким сертификатом в адресной строке отмечают часть доменного имени зеленым цветом (во всех других случаях весь URL-адрес показан серым цветом). Кроме того, при наведении курсора мыши на адрес — — отобразится дополнительная информация о сертификате и его владельце (как правило, для США это город и штат, где размещен сервер). Прохождение реальной проверки указывает на то, что компания, которой принадлежит данный URL-адрес, легитимна и этот факт подтвержден независимым центром сертификации.

Возможно, вы догадываетесь, что браузер на смартфоне отслеживает ваше местонахождение, но, вероятно, вы удивитесь, узнав, что браузер на компьютере делает то же самое. Да, это так. Но как именно это происходит?

Помните, я рассказывал, что в метаданных электронного письма содержатся IP-адреса всех серверов, через которые прошло письмо по пути к получателю? Что ж, снова напомню вам, что IP-адрес, который можно узнать через ваш браузер, может подсказать заинтересованному лицу, какой у вас интернет-провайдер, и сузить область поиска вашего местоположения на карте.

При первом посещении сайта, который специально запрашивает, где вы находитесь (например, сайт с прогнозом погоды), браузер должен спросить у вас, готовы ли вы делиться своим местонахождением с данным сайтом. Если вы согласитесь, то сайт будет автоматически под вас подстраиваться, что очень удобно. Например, сайт **WashingtonPost.com** будет показывать рекламу компаний, расположенных в вашем городе, а не в округе Колумбия.

Не помните, что вы выбрали в прошлый раз? Попробуйте зайти на страницу **benwerd.com/lab/geo.php**. Это один из множества сайтов, позволяющих проверить, сообщает ли ваш браузер геолокационные данные. Если сообщает, а вы хотите быть невидимым, отключите эту опцию. К счастью, в браузере можно отключить отслеживание местоположения. В адресной строке браузера Firefox нужно набрать **about: config**. Выполните поиск, найдите пункт **geo.enabled** и присвойте ему значение **false**. Закройте вкладку. В браузере Chrome нажмите кнопку: и выберите команду **Настройки** (Options). Щелкните мышью по строке **Дополнительные** (Under the Hood) и выберите пункт **Настройки контента — > Геоданные** (Content Settings — > Location). На этой вкладке вы найдете переключатель **Спрашивать разрешение на доступ** (Do not allow any site to track my physical location). Установите переключатель в неактивное положение, чтобы отключить геолокацию. В других браузерах присутствует аналогичная возможность.

Также вы, возможно, захотите сфальсифицировать данные о своем местоположении — разумеется, исключительно ради забавы. Если вы хотите предоставить ложные координаты — например, Белого дома — браузеру Firefox, можно скачать и установить расширение под названием **Change Geolocation**. В браузере Google Chrome существует встроенная функция изменения геоданных. Откройте Chrome и нажмите сочетание клавиш **Ctrl+Shift+I** (Windows) или  (macOS), чтобы открыть окно **Инструменты разработчика** (Developer Tools). Нажмите кнопку  в верхнем правом углу появившейся панели, чтобы открыть меню (не основное меню браузера, а меню панели с инструментами разработчика!). В открывшемся меню выберите пункт **More Tools —> Sensors**. Перейдите на открывшуюся вкладку Sensors и найдите раскрывающийся список **Geolocation**. Выполнив эти действия, можно указать точную широту и долготу. Можно взять известную географическую точку или выбрать координаты посреди океана. В любом случае сайт не узнает, где вы на самом деле находитесь.

Можно скрывать не только физическое местонахождение, но и IP-адрес. Ранее я говорил про программу Tor Browser, которая меняет IP-адрес, передаваемый просматриваемому сайту. Но не все сайты можно посетить через Tor. До недавних пор нельзя было зайти на Facebook. Если вы хотите скрыть свой IP-адрес от сайтов, не поддерживающих соединения через Tor, воспользуйтесь прокси-сервером.

Открытый прокси-сервер — это посредник между вами и Интернетом. В главе 2 я рассказывал о том, что прокси-сервер похож на переводчика с иностранного языка — вы разговариваете с переводчиком, а тот в свою очередь разговаривает с иностранцем, — с той лишь разницей, что ваше сообщение никак не меняется.

Я упоминал прокси-сервер, объясняя, как некий злоумышленник из враждебной страны может попытаться отправить вам электронное письмо, притворяясь сотрудником компании-партнера.

С помощью прокси-сервера также можно заходить на веб-сайты, запрещенные на той или иной территории: например, если вы живете в стране, где запрещен поисковый сайт Google. Или если вы

хотите скрыть свою личность, скачивая через пиринговые сети незаконный или защищенный авторским правом контент.

Однако прокси-сервер не обеспечивает стопроцентной защиты. Каждый браузер необходимо вручную настроить на обращение к прокси-серверу. Разработчики даже лучших прокси признаются, что с помощью определенных трюков, использующих Flash или JavaScript, можно вычислить реальный IP-адрес — т. е. тот, с которого вы подключаетесь к прокси-серверу. Чтобы избежать этого, можно заблокировать или ограничить поддержку Flash и JavaScript в браузере. Лучший способ помешать JavaScript-сценарию отследить вас через браузер — пользоваться расширением HTTPS Everywhere (см. выше).

Существует множество платных прокси-серверов. Но необходимо внимательно читать политику конфиденциальности любого сервиса, на котором вы регистрируетесь. Обращайте внимание, как сервис шифрует передаваемые данные и насколько скрупулезно соблюдает законы и выполняет государственные требования, связанные с предоставлением информации.

Можно найти бесплатные прокси-серверы, но вам придется иметь дело с лавиной бесполезной рекламы.

Что касается меня, то я советую вам избегать бесплатных прокси. В ходе своей презентации на конференции DEF CON20 мой друг и специалист по безопасности Чема Алонсо создал собственный прокси-сервер, чтобы наглядно продемонстрировать, как он может пригодиться злоумышленникам, и прорекламировал его адрес на форуме . Через несколько дней этим бесплатным «анонимным» прокси пользовались уже свыше 5000 человек. К сожалению, большинство из них были мошенниками.

Мораль этой истории — когда сервис бесплатен, вы получаете ровно то, за что заплатили.

Алонсо же, в свою очередь, с помощью этого прокси-сервера также мог без труда внедрить вредоносное ПО в браузер злоумышленника и отслеживать его действия. Так он и поступил, применив метод захвата с помощью BeEF, фреймворка, эксплуатирующего уязвимости браузеров. Кроме того, Алонсо записал в пользовательском соглашении, что оставляет за собой право это сделать. Пользователи были вынуждены *принять* условия соглашения, иначе не смогли бы пользоваться сервисом. Именно благодаря этому Алонсо смог читать электронные письма, пересылаемые через его прокси, и просматривать весь остальной трафик, связанный с преступной деятельностью пользователей. Мораль этой истории — когда сервис бесплатен, вы получаете ровно то, за что заплатили.

Если вы применяете прокси-сервер в сочетании с HTTPS, правоохранительные органы и спецслужбы смогут увидеть только IP-адрес прокси-сервера, но не ваши действия на сайте — эта информация будет зашифрована. Как уже говорилось, обычный HTTP-трафик не зашифрован, поэтому следует всегда пользоваться HTTPS Everywhere (да, это мой ответ на большинство вопросов, связанных с уязвимостями браузера).

Для удобства люди часто синхронизируют настройки браузеров на разных устройствах. Например, когда вы входите в Chrome (авторизовавшись через аккаунт Google) или включаете хромбук, ваши закладки, вкладки, история и остальные настройки браузера синхронизируются через аккаунт Google. Эти настройки автоматически загружаются каждый раз, когда вы запускаете Chrome на обычном компьютере или на мобильном устройстве. Чтобы выбрать, какие данные необходимо синхронизировать с аккаунтом, или настроить шифрование, перейдите в раздел настроек в Chrome. Личный кабинет Google предоставляет полный доступ к управлению информацией, если вы вдруг решите отказаться от синхронизации. Проверьте, чтобы была отключена автоматическая синхронизация конфиденциальных сведений. У браузера Mozilla Firefox также есть возможность синхронизации.

Подвох в том, что хакеру нужно всего лишь заставить вас авторизоваться в аккаунте Google в браузере Chrome или Firefox, после чего вся ваша история поиска будет загружена на его устройство. Представьте себе, что за вашим компьютером посидел ваш друг, который вошел в свой аккаунт. История поиска, закладки и другие данные вашего друга будут синхронизированы. Другими словами, вся эта информация теперь будет видна на вашем компьютере. Кроме того, если вы войдете в синхронизированный аккаунт на компьютере и забудете выйти, все ваши закладки и история браузера будут видны следующему пользователю. Когда вы входите в Google Chrome, отображается информация из абсолютно всех сервисов Google, включая Google Календарь, YouTube и другие. Если вам пришлось выйти в Интернет с такого компьютера, обязательно выйдите из своего аккаунта по завершении работы.

Еще один недостаток синхронизации заключается в том, что на всех связанных друг с другом устройствах будет отображаться один и тот же контент. Если вы живете один, в этом нет ничего страшного. Но если у вас общий с кем-то аккаунт iCloud, может случиться неприятность. Например, родители, которые разрешают детям пользоваться своим планшетом iPad, могут ненароком

познакомить их с контентом для взрослых.

Эллиот Родригес, делопроизводитель из Денвера, штат Колорадо, купив себе новый планшет в магазине Apple, подключил его к своему старому аккаунту iCloud. Все фотографии, сообщения, музыка и видео со старого планшета тут же загрузились на новый. Он сэкономил массу времени, поскольку ему не пришлось вручную переносить все данные на новое устройство. И у него всегда был доступ ко всем материалам, каким бы устройством он ни пользовался.

Через какое-то время Эллиот решил отдать старый планшет своей восьмилетней дочери. Устройства Эллиота и его дочки были подключены к одному и тому же аккаунту iCloud, что было довольно удобно. Время от времени Эллиот замечал новые приложения, установленные дочкой на свой планшет. Иногда они даже отправляли друг другу семейные фотографии. Затем Эллиот поехал в очередную командировку в Нью-Йорк.

Без задней мысли Эллиот снял на свой iPhone несколько фотографий со своей нью-йоркской любовницей, некоторые из которых были довольно… интимными. Фотографии с его iPhone автоматически синхронизировались с планшетом iPad его дочери в Колорадо. И, конечно же, дочка спросила у мамы, что это за женщина с папой. Нужно ли говорить, что Эллиота дома ждало серьезное разбирательство?

Также всплывает проблема подарков ко дню рождения. Если у вас общее устройство или синхронизированные аккаунты, история вашего поиска и просмотренные сайты могут подсказать человеку, что он получит на день рождения. Или, хуже того, мог бы получить. Опять же общий компьютер или планшет в семье может нарушить личное пространство человека.

Один из способов этого избежать — разграничить пользователей, что довольно просто сделать в Windows. Оставьте за собой права администратора, чтобы вы могли управлять параметрами системы, и настройте отдельные дополнительные учетные записи для членов семьи. Каждый будет входить под собственным паролем, и у каждого будет доступ только к собственному контенту, закладкам и истории в браузере.

Операционная система macOS компании Apple также позволяет произвести подобное разграничение. Однако лишь немногие вспоминают о том, что надо бы разделить пользователей в аккаунте iCloud. И иногда, казалось бы, совершенно не по нашей вине мы становимся жертвами предательства со стороны наших же устройств.

Телепродюсер из Лос-Анджелеса Дилан Монро, долгие годы встечаясь с разными женщинами, наконец нашел «ту самую» и решил остепениться. Его невеста переехала к нему, и в честь начала совместной жизни Дилан беспечно подключил свою будущую жену к своему аккаунту iCloud.

Когда вы хотите создать семью, довольно логично подключиться к общему аккаунту. Так можно делиться со своими любимыми видео, музыкой и информацией. Это что касается настоящего. Ну а как насчет вашего цифрового прошлого?

Иногда автоматическое создание резервных копий облачными сервисами типа iCloud приводит к тому, что у нас появляется архив фотографий, музыки и текстов за долгие годы, о некоторых из них мы забываем, как и о содержимом старых коробок на чердаке.

В первую очередь нельзя забывать о фотографиях. И да, многие поколения супругов находили коробки из-под обуви, наполненные старыми письмами и фотографиями. Но изображения высокого разрешения на цифровом носителе, где можно без проблем хранить и просматривать тысячи фотографий, стали новым источником проблем. Внезапно старые воспоминания Дилана — некоторые из которых были довольно личными — настигли его, материализовавшись в виде фотографий на устройствах iPhone и iPad его невесты.

Теперь появилась необходимость убрать из дома некоторые предметы мебели, потому что этот диван, стол или кровать были связаны с интимными моментами Дилана с другими женщинами. И теперь появились рестораны, в которые невеста отказалась ходить, поскольку видела фотографии Дилана в компании других женщин в этих ресторанах: за тем столиком у окна или в той угловой кабинке.

Влюбленный Дилан выполнял все ее требования, даже когда она попросила его о самой большой жертве — продать свой дом после свадьбы. И все из-за того, что он подключил свой iPhone к ее.

Облачный сервис порождает еще одну интересную проблему. Даже если вы очистите историю посещений в браузере на своем настольном компьютере, ноутбуке или мобильном устройстве, резервная копия истории поисковых запросов сохранится в «облаке». Историю, которая хранится на серверах компании-владельца поисковой системы, удалить немного труднее, а еще сложнее сделать так, чтобы она вообще не сохранялась. Вот всего лишь один из примеров того, как тайно собранные данные без должного контекста впоследствии легко могут оказаться перевернутыми с ног на голову. Несложно заметить, как список невинных поисковых запросов может быть

истолкован абсолютно превратно.

Одним летним утром 2013 года, всего через несколько месяцев после взрыва на Бостонском марафоне, муж Мишель Каталано увидел, как напротив их дома в районе Лонг-Айленда припарковались два черных внедорожника. Когда он вышел поздороваться с офицерами, они попросили у него документы и спросили, могут ли они осмотреть дом. Мужчине было нечего скрывать, поэтому он впустил их, хотя и не мог понять, чем их так заинтересовал его дом. Бегло осмотрев комнаты, федеральные агенты перешли к сути: «Кто-нибудь в этом доме искал в Интернете информацию о скороварках? А о рюкзаках?»

По всей видимости, запросы членов семьи в поисковой системе Google привлекли внимание Министерства внутренней безопасности США, которое инициировало предварительное расследование. В отсутствие информации о том, как на самом деле происходило расследование по делу семьи Каталано, остается лишь предположить, что несколько месяцев после взрыва на Бостонском марафоне сочетание определенных поисковых запросов рассматривалось как возможная подготовка теракта, поэтому предпринимались меры. Через два часа подозрения в отношении Каталано были развеяны. Позже Мишель описала этот случай в блоге на сайте Medium — только в качестве предостережения о том, что ваш сегодняшний интернет-поиск завтра может вылиться в проблему.

В своей статье Каталано отметила, что спецслужбы почему-то сбросили со счетов поисковые запросы «Как готовить чертову квиноу?» и «Алекс Родригес до сих пор отстранен?». Она сказала, что искала скороварку для приготовления квинои. А рюкзак? Ее мужу нужен был рюкзак.

Как минимум одна компания, владелец поисковой системы — Google, создала несколько инструментов для настройки приватности аккаунта, с помощью которых можно обозначить, какую информацию можно сохранять, а какую — нет. Например, можно отключить отслеживание в рекламных целях, чтобы вам после просмотра информации о Патагонии не стали показывать рекламу туров в Южную Америку. Также можно вообще отключить сохранение истории поиска. Или же можно не авторизоваться в Gmail, YouTube и любом другом сервисе аккаунта Google, пока вы что-то ищете в Интернете.

Даже если вы не авторизованы в своей учетной записи Microsoft, Yahoo! или Google, все равно к каждому поисковому запросу привязан ваш IP-адрес. Один из способов избежать этой привязки — пользоваться прокси компании Google (**startpage.com**) или поисковой системой DuckDuckGo.

DuckDuckGo — это поисковая система, по умолчанию предпочитаемая в браузерах Firefox и Safari. В отличие от Google, Yahoo! и Microsoft, в поисковой системе DuckDuckGo отсутствуют учетные записи пользователей, а сайт компании сообщает, что перед вами «поисковая система, которая не отслеживает вас». У компании также есть свой выходной узел Tor, а следовательно, вы можете пользоваться поиском DuckDuckGo при работе с Tor, не ощутив при этом никаких неудобств.

Поскольку сайт DuckDuckGo не отслеживает вашу активность, результаты поиска не будут фильтроваться в соответствии с предыдущими поисковыми запросами. Большинство людей этого не осознают, но на результаты поиска Google, Yahoo! и Bing влияют все ваши предыдущие поисковые запросы в данной конкретной системе. Например, если поисковая система видит, что вас интересуют сайты с медицинской тематикой, она отфильтрует поисковые результаты, поставив на первые строчки те из них, которые относятся к медицине. Почему? Потому что мало кто из нас утруждает себя переходом на вторую страницу с результатами поиска. На эту тему даже появилась шутка: лучшее место, чтобы спрятать труп — вторая страница результатов поиска.

Некоторые люди решат, что отсутствие необходимости пролистывать неподходящие результаты поиска — это удобно, но в то же самое время вы наделяете поисковую систему полномочиями решать, что вам будет интересно, а что нет.

По большому счету это цензура.

Некоторые люди решат, что отсутствие необходимости пролистывать неподходящие результаты поиска — это удобно, но в то же самое время вы наделяете поисковую систему полномочиями решать, что вам будет интересно, а что нет. По большому счету это цензура. DuckDuckGo показывает релевантные поисковые результаты, но ориентируется при этом на сам запрос, а не на историю вашего поиска.

В следующей главе я расскажу о том, как сайты пытаются помешать вам стать для них невидимым и что можно сделать, чтобы путешествовать по Интернету анонимно.

Глава 6

Я БУДУ СЛЕДИТЬ ЗА КАЖДЫМ ЩЕЛЧКОМ ТВОЕЙ МЫШИ

Будьте очень внимательны, когда ищете что-то в Интернете. Вашу активность в Интернете отслеживают не только поисковые системы, но и каждый веб-сайт, который вы посещаете. Причем некоторые из них, казалось бы, не должны разглашать конфиденциальную информацию. Например, согласно выпущенному в 2015 году отчету, 70 процентов медицинских сайтов отображают личную медицинскую информацию, включая конкретные болезни и методы лечения, прямо в URL страницы.

Другими словами, если я на портале WebMD ищу информацию об *эпидермофитии стоп*, зашифрованная фраза «эпидермофития стоп» отобразится в URL в адресной строке моего браузера. Это означает, что кто угодно — браузер, интернет-провайдер, оператор сотовой связи — может увидеть, что я ищу информацию об эпидермофитии стоп. Если в браузере установлено расширение HTTPS Everywhere и просматриваемый сайт поддерживает HTTPS, читаемый вами контент будет зашифрован, но URL — нет. Как уточнили в Фонде электронных рубежей, в задачи HTTPS никогда не входило сокрытие данных о том, какие сайты вы посещаете.

Будьте очень внимательны, когда ищете что-то в Интернете. Вашу активность в Интернете отслеживают не только поисковые системы, но и каждый веб-сайт, который вы посещаете. Причем некоторые из них, казалось бы, не должны разглашать конфиденциальную информацию.

Кроме того, проведенное исследование выявило, что 91 % сайтов с медицинской тематикой сами отправляют запросы сторонним ресурсам. Эти запросы встроены в страницы, они обращаются к крошечным изображениям (которые могут быть видны, а могут быть и нет), которые сообщают сторонним ресурсам, что вы посетили определенную страницу. Введите в поиск фразу «эпидермофития стоп», и целых двадцать различных сайтов — от фармацевтических ресурсов до сайтов типа Facebook, Pinterest, Twitter и Google — будут в курсе того, какие результаты поиска были загружены в вашем браузере. Теперь все эти сайты знают, что вы искали информацию об эпидермофитии стоп.

Сторонним сайтам нужна эта информация, чтобы настроить показ контекстной рекламы. Помимо этого, если вы авторизовались на сайте медицинской тематики, они также могут получить ваш электронный адрес. К счастью, я могу подсказать вам, как помешать этим организациям получить дополнительные данные.

По данным исследования, проведенного в 2015 году, был составлен список десяти сторонних организаций: Google, comScore, Facebook, appNexus, AddThis, Twitter, Quantcast, Amazon, Adobe и Yahoo!. Часть из них — comScore, appNexus и Quantcast — занимаются учетом интернет-трафика, как и Google. Из перечисленных выше сторонних организаций Google, Facebook, Twitter, Amazon, Adobe и Yahoo! шпионят за вами из коммерческих соображений, например, чтобы в будущем показывать вам рекламу на тему лечения эпидермофитии стоп.

Также в исследовании упоминаются ресурсы Experian и Axiom, которые представляют собой просто хранилища данных: они собирают столько данных о человеке, сколько могут. А затем продают их. Помните, мы говорили о секретных вопросах и о том, что лучше выдумывать ответы на них? Часто компании, такие как Experian и Axiom, собирают, передают и обрабатывают эти секретные вопросы, создавая на их основе профили интернет-пользователей. Эти профили представляют большой интерес для маркетологов, которым необходимо рекламировать продаваемые товары определенным социальным группам.

Как это работает?

Независимо от того, набираете ли вы URL вручную или переходите на ресурс через поисковую систему, у каждого сайта в Интернете есть и доменное имя, и числовой IP-адрес (у некоторых сайтов есть только числовой адрес). Однако числовой адрес практически никогда не отображается. Браузер его скрывает, обращаясь к службе доменных имен (англ. Domain Name System, DNS), которая преобразует буквенный адрес, например Google, в числовой, в данном случае .

DNS — это всемирная телефонная книга, с помощью которой можно связать числовой адрес сервера, на котором размещен запрашиваемый сайт, с его доменным именем. Например, если набрать в адресной строке браузера **Google.com**, DNS свяжется с сервером по адресу , и вы увидите белый экран с логотипом Google и пустой поисковой строкой. Теоретически именно так работают все веб-браузеры. На практике все происходит несколько иначе.

После того как сайт был идентифицирован по своему числовому адресу, он отправляет веб-браузеру данные, чтобы запустить процесс отображения веб-страницы. Браузер в ответ на свой вопрос получает страницу, содержащую элементы, которые вы ожидаете увидеть — информацию, которая вас интересует, изображения по теме и элементы для перехода на другие страницы сайта. Однако

часто на полученной браузером странице присутствуют элементы, которые инициируют переход на другие сайты с дополнительными изображениями или сценариями. Некоторые из этих сценариев (если не все) выполняют функцию отслеживания ваших действий, и в большинстве случаев вам они совершенно не нужны.

Почти у всех цифровых технологий есть метаданные, и, как вы, безусловно, уже догадались, браузеры не исключение.

Ваш браузер может дать просматриваемому веб-сайту множество сведений о вашем компьютере. Например, какой версией какого браузера вы пользуетесь, какая у вас операционная система, какие расширения браузера вы установили, а также какие еще программы запущены на вашем компьютере в данный момент (например, продукты Adobe). По этим метаданным можно даже установить технические характеристики компьютера, например, разрешение экрана и объем встроенной памяти.

Возможно, прочитав книгу до этой страницы, вы уже считаете, что предприняли все необходимые меры для того, чтобы стать невидимым в Интернете. И это так. Но необходимо сделать кое-что еще.

Уделите немного времени и зайдите на сайт **Panopticlick.com**. Этот ресурс, созданный Фондом электронных рубежей, определит, насколько типична или уникальна конфигурация вашего браузера по сравнению с другими, в зависимости от программного обеспечения вашего компьютера или мобильного устройства, а также от того, какие плагины вы могли установить. Т. е. установлены ли у вас какие-либо плагины, с помощью которых можно как-то ограничить круг данных, которые сайт Panopticlick.com сумеет получить от браузера.

Если среди результатов тестирования Panopticlick вы увидите много зеленых галочек, ваш браузер довольно уникален, поскольку сильно защищен. Поздравляю! Но если вы видите больше красных крестиков, настройки вашего браузера достаточно типичны. Это значит, что, если я захочу настроить для вас показ рекламы или рассылку вредоносного ПО, мне не придется сильно напрягаться, потому что у вас довольно обычный браузер с очень распространенными настройками.

Вероятно, вы считаете, что типичные настройки играют вам на руку, делая вас невидимым — вы сливаетесь с толпой, вы ее часть. Но с технической точки зрения такие настройки делают вас легкой мишенью для злоумышленников. Хакеру не хочется тратить слишком много усилий. Если в одном доме дверь открыта, а в соседнем — закрыта, какой из них, как вы думаете, выберет грабитель? Если хакер выяснит, что у вас обычные настройки, то, скорее всего, вы также не предприняли никаких защитных мер, которые могли бы вас обезопасить.

Мы довольно резко перепрыгнули от рекламодателей, которые пытаются выяснить, что вас интересует в Интернете, к хакерам, которые могут воспользоваться вашими персональными данными в целях кражи вашей личности. Это совершенно разные вещи. Рекламодателям нужна информация для создания рекламы, благодаря которой сайт будет приносить доход. Без рекламы некоторые сайты просто не смогут оставаться на плаву. Однако рекламодатели, хакеры и даже спецслужбы стараются узнать о вас то, что, возможно, вы не хотите разглашать. Поэтому с точки зрения информационной безопасности все они представляют для вас одинаковую угрозу.

Один из способов слиться с толпой, но при этом избежать интернет-прослушки — виртуальная машина, отдельная программная система, например Linux, на базе основной операционной системы вашего компьютера, например Windows. На компьютер можно установить какой-нибудь из продуктов VMWare, чтобы при необходимости запускать другую операционную систему.

По завершении работы просто закройте программу. Операционная система исчезнет вместе со всем, что вы в ней делали (кроме сохраненных вами файлов, которые останутся там, где вы их сохранили).

Еще один распространенный прием, который одинаково часто применяют как хакеры, так и рекламодатели, заключается в сборе информации о посетителях сайта с помощью однопиксельных изображений или веб-маячков (веб-жучков, web bug). Как и всплывающее пустое окно браузера, однопиксельное изображение размещается на странице и, будучи невидимым, обращается к стороннему сайту, поместившему его в это место. Сервер, на котором хранится «маячок», фиксирует, с какого IP-адреса он был запрошен. «Маячок» на медицинском сайте поделится с ним информацией о том, что я интересовался лекарствами от эпидермофитии стоп.

Упомянутое выше исследование 2015 года показало, что почти половина обращений к сторонним сайтам приводит к созданию всплывающего окна без какого-либо контента. Эти «пустые» окна скрытно отправляют HTTP-запросы сторонним серверам исключительно с целью отслеживания трафика. Чтобы этого избежать, запретите браузеру открывать любые всплывающие окна (так вы заодно избавитесь от надоедливой рекламы).

Примерно треть оставшихся сторонних запросов, согласно исследованию, представляют собой

короткие строки кода, файлы JavaScript, которые обычно просто запускают на странице анимацию. Веб-сайт может идентифицировать компьютер, получивший к нему доступ, с помощью IP-адреса, с которого запрашивается JavaScript-файл.

Даже без однопискельных изображений и пустых всплывающих окон каждый посещенный сайт может отследить ваш путь в Интернете. Например, Amazon может узнать, что вы только что были на медицинском сайте, и предложить вам медицинские товары. Информация о ресурсе, который вы только что посетили, содержится в запросе, отправляемом вашим браузером сайту Amazon.

Amazon выполняет это, используя сторонние рефереры — данные в текстовом виде в запросе, отправляемом веб-странице. Они сообщают новой странице, откуда исходит запрос. Например, если я читаю статью на сайте Wired и в этой статье содержится ссылка, когда я щелкну по этой ссылке, новый сайт будет знать, что до этого я посетил страницу на ресурсе **Wired.com**. Можно догадаться, как подобное отслеживание переходов сказывается на конфиденциальности.

Чтобы это предотвратить, можно всегда заходить на **Google.com** и уже оттуда открывать другой сайт, чтобы ни один из ресурсов не знал, где вы были до этого. Лично я не считаю, что следует слишком переживать из-за реферальных данных, за исключением тех случаев, когда вы хотите скрыть свою личность. Опять же ради невидимости придется терпеть некоторое неудобство: вместо того чтобы просто перейти на следующий сайт, вам придется всегда стартовать с **Google.com**.

У браузера Mozilla Firefox есть одно из лучших средств защиты против отслеживания трафика третьими сторонами — расширение под названием NoScript. Этот плагин эффективно блокирует практически все, что потенциально способно навредить компьютеру и браузеру, в частности Flash и JavaScript. Расширения для дополнительной защиты меняют сценарий работы с браузером, хотя можно выбирать только те настройки, которые вам подходят, или же указать сайты, которым вы доверяете.

Установив расширение NoScript, вы обратите внимание, что на просматриваемых страницах не будет рекламных объявлений, и уже точно сайты не будут получать реферальные данные. Результатом блокировки нежелательных элементов станет также то, что внешне страница станет немного менее пестрой, чем раньше. Если вам вдруг захочется посмотреть видео в формате Flash в верхнем левом углу страницы, можно разрешить загрузиться этому элементу без разблокировки остальных. Или же, если вам кажется, что сайт заслуживает доверия, можно временно или навсегда разрешить загружаться всем элементам страницы — например, если это сайт банка.

В браузере Chrome можно установить расширение ScriptBlock, которое в целях защиты блокирует выполнение любых скриптов на странице. Это удобно, когда у вас есть дети, которые могут зайти на сайт с всплывающими окнами, содержащими контент для взрослых.

Блокировка потенциально опасных (и уж точно нарушающих конфиденциальность) элементов на этих страницах оградит компьютер от нежелательного рекламного программного обеспечения. Например, возможно, вы заметили, что на домашней странице Google появилась реклама. На самом деле на вашей домашней странице Google не должно быть всплывающей рекламы. Если вы видите такую рекламу, значит, ваш компьютер и браузер были скомпрометированы (возможно, когда-то давно), а то, что вы видите теперь, — это объявления сторонних рекламодателей, которые могут заразить ваш компьютер троянами, клавиатурными шпионами и прочими вредоносными программами, если вы по ним щелкнете. Даже если в объявлении нет вредоносных программ, доход размещающих их сайтов зависит от количества щелчков по ним. Чем больше людей кликнут по объявлению, тем больше денег оно принесет владельцу.

Какими бы эффективными они ни были, NoScript и ScriptBlock не могут заблокировать абсолютно все. Для обеспечения полной защиты от других угроз можно установить дополнение AdBlock Plus. Единственная проблема заключается в том, что AdBlock все фиксирует, а значит, еще одна компания будет отслеживать историю вашей активности в Интернете, несмотря на все ваши попытки сохранить анонимность. И все же в этом случае плюсы (блокировка потенциально опасных рекламных объявлений) перевешивают минусы (кто-то узнает, что вы делали в Интернете).

Еще одно полезное расширение называется Ghostery, его можно установить как на Chrome, так и на Firefox. Ghostery выявляет все программы, собирающие информацию о трафике (например, Doubleclick и Google AdSense), которые применяются сайтами для отслеживания ваших действий. Как и NoScript, плагин Ghostery позволяет для каждой страницы выбрать программы, которым вы разрешаете собирать информацию о трафике. На сайте написано: «Блокировка трекеров предотвратит их запуск в браузере, позволив вам контролировать сбор информации о ваших действиях в Интернете. Помните, что некоторые трекеры могут быть полезны, например, виджеты социальных сетей или браузерные игры. Блокировка трекеров может непредсказуемым образом отразиться на работе сайтов, которые вы посещаете». Это означает, что некоторые сайты не будут отображаться при установленном расширении Ghostery. К счастью, Ghostery можно отключать для каждого сайта в отдельности.

Чтобы помешать потенциальным хакерам идентифицировать вас и окончательно сбить их с толку, помимо установки расширений можно также создать несколько отдельных электронных ящиков под разные цели. Например, в главе 2 мы говорили о том, как зарегистрировать анонимный электронный ящик для конфиденциальной переписки. Завести несколько электронных ящиков я рекомендую, даже если вы просто выходите в Интернет: не столько для того, чтобы скрывать свою личность, сколько для того, чтобы стать менее интересной мишенью для третьих лиц. Если у вас будет несколько поведенческих профилей, сведения о вас будут более размытыми, нежели при наличии всего одного ящика, по которому можно установить вашу личность. Составить на вас профиль станет гораздо сложнее.

Представим, что вы захотели купить что-то в Интернете. Возможно, вы решите зарегистрировать отдельный электронный ящик только для интернет-шоппинга. И предположим, все ваши покупки будут доставляться не к вам на дом, а на специальный абонентский ящик до востребования. И допустим, вы оплачиваете покупки подарочными сертификатами (или одним и тем же сертификатом с восполняемым балансом).

В таком случае у компании-продавца будут только ваш второстепенный электронный адрес, второстепенный адрес доставки и данные подарочного сертификата (одноразового или практически одноразового). Если у этой компании произойдет утечка данных, злоумышленники не получат ни вашего настоящего электронного адреса, ни вашего фактического адреса, ни данных банковской карты. Такого рода дистанцирование от процесса совершения покупки в Интернете — это прекрасный способ сохранить конфиденциальность.

Также можно завести отдельный электронный ящик для социальных сетей. Он может выполнять функцию «публичной электронной почты» для общения с незнакомыми и малознакомыми людьми. Преимущество в том, что опять же посторонним людям не удастся узнать о вас много информации. По крайней мере, напрямую.

Чтобы еще сильнее себя защитить, придумайте для каждого «второстепенного» аккаунта уникальное название, например, пусть это будет вариация вашего настоящего имени или что-то совершенно иное.

Не забывайте, что наша задача заключается в том, чтобы слиться с фоном, а не привлечь внимание к собственной персоне.

Выбрав первый вариант, нельзя забывать об осторожности. Полагаем, не следует указывать свое отчество. Даже на первый взгляд безобидный адрес электронной почты, скажем, , выдает, что ваше отчество начинается с буквы В. Это пример того,

как человек сам раскрывает конфиденциальную информацию о себе, когда в этом нет необходимости. Не забывайте, что наша задача заключается в том, чтобы слиться с фоном, а не привлечь внимание к собственной персоне.

Если вы возьмете слово или словосочетание, никак не связанное со своим настоящим именем, пусть оно будет как можно более нейтральным. Если новый ящик имеет адрес , мы не будем знать вашего имени, но узнаем, чем вы увлекаетесь. Лучше выбрать что-то шаблонное, типа .

Конечно же, вам захочется завести электронный ящик для личной переписки. Этот адрес нельзя давать никому, кроме близких друзей и родственников. Все эти меры предосторожности сопровождаются дополнительным преимуществом: вы обнаружите, что, перестав указывать свой личный электронный ящик на сайтах интернет-магазинов, избавитесь от львиной доли спама.

Сотовые телефоны также не застрахованы от шпионажа со стороны крупных корпораций. Летом 2015 года наблюдательный специалист обнаружил, что операторы AT&T и Verizon добавляют дополнительный код к каждому запросу веб-страницы, исходящему от мобильного браузера. Это не идентификатор IMSI (международный идентификатор мобильного абонента), о котором мы говорили в главе 3, а уникальный идентификатор, который отправляется при каждом запросе веб-страницы. Этот код называется UIDH (от англ. Unique Identifier Header — заголовок уникального идентификатора) и представляет собой временный серийный номер, с помощью которого рекламодатели могут пометить вас в Интернете.

Специалист обнаружил этот идентификатор благодаря тому, что настроил анализатор трафика таким образом, чтобы тот сохранял все заголовки (что делают немногие). Затем он обратил внимание на то, что об абонентах Verizon собирается больше данных, чем о других посетителях. А позже понял, что это относится и к абонентам AT&T.

Проблема в том, что пользователи не знали об этом коде. Например, даже если человек скачал на устройство мобильную версию браузера Firefox и установил специальные расширения для информационной безопасности, но при этом он является абонентом AT&T или Verizon, его действия в Интернете все равно будут отслеживаться посредством UIDH.

С помощью идентификаторов UIDH операторам Verizon и AT&T удавалось отслеживать трафик, связанный с запросами пользователей, и либо создавать их поведенческие профили (чтобы впоследствии правильно настроить рекламу), либо просто перепродавать полученные данные.

Оператор AT&T отказался от этой практики — пока. Verizon предоставил своим пользователям право управлять UIDH в настройках. Обратите внимание: если вы не отключили эту настройку, считается, что вы дали Verizon свое согласие на применение UIDH.

Даже если вы отключите JavaScript, просматриваемый сайт может отправить вашему браузеру текстовый файл под названием «куки» (cookie). Этот куки будет храниться долго. Название «куки» — это сокращенный вариант от magic cookie (англ. волшебное печенье), небольшой фрагмент данных, передаваемый браузеру и хранимый на компьютере пользователя для отслеживания таких вещей, как содержимое корзины покупок или даже авторизация пользователя. Изначально куки применялись браузером Netscape и служили для создания электронных корзин и других инструментов интернет-магазинов. Куки обычно сохраняются в браузере компьютера и удаляются через определенное время, хотя этот срок может измеряться десятилетиями.

Опасны ли куки? Сами по себе нет. Тем не менее они передают третьим лицам информацию о вашей учетной записи и настройках для определенного сайта, например, избранные города на сайте с прогнозом погоды или предпочтительные авиакомпании на туристическом сайте. В следующий раз, когда браузер установит соединение с сайтом, для которого у вас уже сохранен куки, тот вспомнит вас и, вероятно, скажет: «Привет, друг». Если же это интернет-магазин, он также вспомнит несколько ваших последних покупок.

Куки на самом деле не хранят эту информацию на компьютере или мобильном устройстве. Как и мобильные телефоны, для которых идентификаторы IMSI выступают в качестве ссылки, в куки содержится лишь ссылка на данные, находящиеся на сервере. Когда браузер загружает страницу, для которой у него сохранен куки, сайт отправляет в ответ дополнительную информацию, связанную с настройками и предпочтениями пользователя.

В куки хранятся не только персональные настройки, но и ценные для сайта статистические данные. Например, если вы потенциальный клиент компании и, чтобы получить доступ к информационным буклетам, уже оставляли на сайте свой адрес электронной почты или другие сведения о себе, велика вероятность, что в вашем браузере присутствует куки, с помощью которого компания может связать ваш профиль с данными из своей CRM-системы (CRM), скажем, SalesForce или HubSpot. Теперь при каждом посещении сайта компании вы будете идентифицированы с помощью куки, хранящегося в вашем браузере, и это посещение также будет отмечено в CRM-системе.

Куки сегментированы, т. е. сайт А обычно не видит содержимое куки сайта Б. Встречаются исключения, но, как правило, данные разделены из соображений безопасности. И все же, если посмотреть на куки с точки зрения интересующей нас темы, они мешают вам стать невидимыми.

Можно получить доступ только к куки с одного домена, группы ресурсов, приписанных определенному кругу людей. Рекламные сети обходят это ограничение, устанавливая один общий куки, который будет соотноситься с вашей деятельностью на всех сайтах сети. Однако в большинстве случаев куки не могут получать доступ к куки других сайтов. Современные браузеры позволяют пользователям соглашаться или отказываться от приема куки, Например, если вы выходите в Интернет в режиме инкогнито или через приватное окно браузера, браузер не сохранит историю ваших действий в эту сессию, а также у вас не появится новых куки (но если у вас уже есть подходящий куки, установленный ранее, он будет использоваться даже в режиме инкогнито). С другой стороны, если вы пользуетесь браузером в обычном режиме, можно время от времени вручную удалять все или некоторые куки, накопившиеся за несколько лет.

Необходимо отметить, что не следует удалять все куки. Выборочно удалив куки, установленные теми сайтами, которые вы посещали лишь однажды и которые вам более не интересны, вы устраните следы своего интернет-серфинга. Например, повторно посещаемые вами сайты не смогут вас идентифицировать. Но что касается других сайтов, например с прогнозом погоды, будет довольно утомительно каждый раз указывать свой город или индекс, в то время как простой cookie-файл сможет избавить вас от этой необходимости.

Чтобы удалить куки, нужно использовать расширение или открыть настройки браузера и найти там команду, предлагающую удалить один или более (даже все) куки. Вы также можете решать, что делать с каждым cookie-файлом по отдельности.

Некоторые рекламодатели с помощью куки также определяют, сколько времени вы провели на сайте, где размещена их реклама. Некоторые даже отслеживают, с какого сайта вы перешли или на каких сайтах вы были ранее. Такие куки нужно удалять сразу же. Вы узнаете их благодаря тому, что их имя не будет совпадать с именем посещенного сайта. Например, вместо CNN такой файл будет значиться как Ad321. Возможно, вам будет удобнее прибегнуть к специальной программе для очистки куки, например **piriform.com/ccleaner**, чтобы быстро и без труда избавиться от ненужных

куки-данных.

Однако существуют куки, на которые не действуют ваши настройки в браузере, которые называются «супер-куки», поскольку они хранятся на компьютере вне браузера. Суперкуки видят ваши персональные настройки (и статистику) для данного сайта вне зависимости от того, каким браузером вы пользуетесь (сегодня Chrome, завтра Firefox). И если вы вдруг удалите такой куки из своего браузера, компьютер попытается его восстановить, когда вы в следующий раз откроете соответствующий сайт.

Два вида таких суперкуки можно удалить в первую очередь — Flash компании Adobe и Silverlight корпорации Microsoft. Эти суперкуки не имеют срока действия и сами никогда не удалятся. Как правило, можно без последствий удалить их все.

Если вы пытаетесь прикинуть, сколько куки уже установлено в вашем браузере, умножьте свое число на потенциальное количество хранилищ данных на вашем компьютере. Увидите, что работы вам хватит на целый день до вечера.

Несколько слов о самом сложном для удаления куки: Сэми Камкар, получивший известность за создание быстро распространяющегося червя MySpace под названием «Сэми», разработал так называемый «evercookie» — очень, очень устойчивый куки. Камкар достиг этой устойчивости благодаря тому, что данные куки стали записываться в максимально большое количество систем хранения браузеров в операционной системе Windows. Если хотя бы в одном из хранилищ файл сохранился, evercookie предпримет попытку восстановить эти куки-данные везде. Таким образом, просто удалить evercookie из кэш-памяти одного браузера недостаточно. По принципу детской игры «Ударь крота», файлы evercookie продолжат появляться то тут, то там. Чтобы выиграть, нужно удалить их абсолютно отовсюду.

Если вы пытаетесь прикинуть, сколько куки уже установлено в вашем браузере, умножьте свое число на потенциальное количество хранилищ данных на вашем компьютере. Увидите, что работы вам хватит на целый день до вечера.

За вашими действиями в Интернете следят не только сайты и операторы сотовой связи. Например, ресурс Facebook давно перестал быть просто социальной сетью и стал универсальной платформой. Можно зарегистрироваться на сайте Facebook, а затем регистрироваться во множестве различных приложений с помощью данных своей учетной записи Facebook.

Насколько часто так поступают? Как минимум один маркетинговый отчет показал, что 88 процентов американских пользователей зашли на сайт или в мобильное приложение с помощью ранее созданного аккаунта в социальной сети, например, Facebook, Twitter и Google+.

Это удобно, но здесь есть как преимущества, так и недостатки. Уязвимость в протоколе авторизации OAuth позволяет получить доступ к другому сайту, не передавая этому сайту логин и пароль от своего аккаунта. С одной стороны, можно быстро зарегистрироваться на новом сайте с помощью существующей учетной записи в социальной сети. С другой стороны, это позволяет социальным сетям получить информацию о вас, которую могут применять в маркетинговых целях. В то же время теперь ресурс будет знать не только то, что вы заходили на этот сайт, но и все остальные сайты, которые вы посетили с помощью тех же регистрационных данных. При использовании протокола OAuth мы жертвуем слишком большим количеством персональной информации ради удобства.

Facebook, вероятно, можно назвать самой «навязчивой» социальной платформой. Выход из аккаунта Facebook может привести к автоматическому выходу из всех остальных приложений. Кроме того, Facebook подключает трекеры для отслеживания действий пользователя, которые функционируют даже после того, как вы вышли из учетной записи, запрашивая такие данные, как ваше географическое местонахождение, посещенные вами сайты, элементы, по которым вы щелкнули на этих сайтах, и ваше имя на сайте Facebook. Специалисты по информационной безопасности выразили беспокойство относительно того, что сайт Facebook намеревается собирать статистику некоторых из посещаемых его пользователями ресурсов и приложений, чтобы повысить релевантность рекламы.

Суть в том, что Facebook, как и Google, хочет получить сведения о вас. Они не могут просто прийти и задать вопрос, им приходится искать другие пути. Если вы привяжете аккаунт Facebook к другим сервисам, у Facebook будет информация о вас и о всех тех сервисах или приложениях. Возможно, с помощью регистрационных данных Facebook вы получаете доступ к своему банковскому счету, в этом случае у социальной сети есть сведения о том, какую финансовую организацию вы выбрали.

Авторизация через Facebook может привести к тому, что, если кто-то проникнет в ваш аккаунт в этой социальной сети, он получит доступ ко всем связанным с ним сайтам, даже к банковскому счету. С точки зрения безопасности, наличие так называемой единой точки отказа никогда не доводит до добра. Пусть на это уйдет на пару секунд дольше, лучше авторизоваться на сайте Facebook только тогда, когда вам нужен именно он, а в каждом приложении регистрироваться по

отдельности.

Кроме того, Facebook открыто признает, что не поддерживает функцию Do Not Track (англ. «Не отслеживать») браузера Internet Explorer на том основании, что на ее счет «в отрасли нет единого мнения». В качестве инструмента сбора статистики Facebook применяет классические средства: куки, JavaScript, однопиксельные изображения и плавающие фреймы. Благодаря всему этому рекламодатели могут просматривать и анализировать куки и трекеры конкретного браузера, чтобы предлагать свои товары и услуги на сайте Facebook и за его пределами.

К счастью, для браузеров существуют расширения, которые блокируют службы Facebook на сторонних сайтах, например, Facebook Disconnect для браузера Chrome или список Facebook Privacy List расширения Adblock Plus (как для браузера Firefox, так и для Chrome). Конечная цель всех этих средств одна — позволить вам самостоятельно контролировать, какие данные будет получать Facebook и любая другая социальная сеть, вместо того чтобы отойти в сторону и оставить решение этого вопроса в руках самого сервиса.

Учитывая то, какими сведениями Facebook располагает о 2,13 млрд своих подписчиков, компания до сих пор проявляла исключительное великодушие. В ее распоряжении тонны данных, но она, подобно компании Google, предпочитает ничего с ними не делать. Но это не значит, что не станет в будущем.

Не менее беспардонно, но более открыто (по сравнению с куки) действуют панели инструментов. Дополнительные панели инструментов, которые вы видите в верхней части браузера на своем компьютере, могут называться Yahoo! McAfee, Яндекс или Ask.com. Или как угодно еще. Вполне вероятно, что вы даже не вспомните, как эта панель инструментов сюда попала. Вам она не нужна, но как ее убрать, вы не знаете.

Такие панели инструментов отвлекают внимание от панели инструментов самого браузера, с помощью которой можно выбрать поисковую систему по умолчанию. «Паразитическая» панель станет навязывать вам свою систему, и результаты поиска могут быть переполнены проплаченным контентом. В такой ситуации оказался житель Западного Голливуда Гэри Мур, который обнаружил у себя панель инструментов Ask.com и не мог понять, как от нее избавиться. «Это как незваный гость, — сказал Мур. — Он не уйдет».

Если у вас появилась вторая или третья панель инструментов, возможно, дело в том, что вы скачали новое программное обеспечение или обновили ранее установленное. Например, если на компьютере установлена среда разработки или исполнения языка Java, компания Oracle, разработчик Java, автоматически встраивает в браузер панель инструментов, если вы не сбросили соответствующий флажок при загрузке. Щелкая по кнопкам загрузки или обновления, вы, вероятно, не заметили крошечный флажок, по умолчанию подтверждающий ваше согласие на установку панели типа Ask.com. Тут нет ничего противозаконного, вы разрешили это действие, даже если разрешением считается то, что вы не отказались от автоматической установки данного элемента. Однако такая панель позволяет некой компании отслеживать ваши действия в Интернете, и, вероятно, по умолчанию у вас теперь выбрана соответствующая поисковая система.

Лучший способ удалить панель инструментов — деинсталлировать ее так же, как деинсталлируется любая другая программа на компьютере. Однако для удаления некоторых наиболее устойчивых и настырных панелей, может понадобиться специальная программа, и нередко после деинсталляции остается достаточно данных для того, чтобы рекламодатели могли установить свою панель заново.

Устанавливая новое программное обеспечение или обновляя старое, обращайте внимание на каждый флажок. Можно избежать большого объема лишней работы, отказавшись от установки панелей инструментов с самого начала.

Если вы пользуетесь анонимным режимом браузера, расширениями NoScript и HTTPS Everywhere, время от времени удаляете куки и лишние панели инструментов, у вас все должно быть в порядке, верно? Отнюдь. Ваши действия в Интернете все равно будут отслеживаться.

Если вы пользуетесь анонимным режимом браузера, расширениями NoScript и HTTPS Everywhere, время от времени удаляете куки и лишние панели инструментов, у вас все должно быть в порядке, верно? Отнюдь. Ваши действия в Интернете все равно *будут* отслеживаться.

Веб-сайты создаются с помощью так называемого языка разметки гипертекста, или HTML. Его актуальная версия, HTML5, предоставляет множество новых возможностей. Некоторые возможности способствовали вытеснению технологий Silverlight и Flash — что хорошо. Однако, вероятно, случайно язык HTML5 привел к появлению новых технологий сбора статистики.

Например, Canvas fingerprinting — инструмент сбора данных в Интернете, гениальный, но гениальность такого рода внушает страх. Canvas fingerprinting использует элемент canvas HTML5 для того, чтобы нарисовать простое изображение. И все. Изображение создается внутри самого

браузера, а вы этого не видите. Процесс занимает всего долю секунды, но его результат доступен запрашивающему сайту.

Смысл в том, что программное обеспечение и аппаратные средства, выступая в качестве ресурсов для работы браузера, создадут совершенно уникальное изображение. Затем получившееся изображение (это может быть последовательность различных разноцветных фигур) преобразуется в уникальное число, примерно как в случае с паролями. Далее проводится анализ, какие еще сайты получили то же самое число, используя эту технологию. И на основании полученных данных можно понять, какие сайты вы посещаете. Благодаря полученному числу или «отпечатку» запросивший его сайт может узнавать браузер пользователя, который уже бывал на нем ранее, даже если пользователь удалил все куки или запретил установку новых cookie-файлов, поскольку он использует элемент самого HTML5.

Canvas fingerprinting работает в фоновом режиме, вам не надо ни на что нажимать, достаточно просто открыть страницу. К счастью, существуют расширения для браузера, которые могут заблокировать это действие. Для браузера Firefox расширение называется CanvasBlocker. Для Google Chrome — CanvasFingerprintBlock. Даже в Tor Browser разработчики добавили технологию блокировки Canvas.

Так что же, благодаря этим расширениям и предыдущим рекомендациям, вы наконец можете считать, что в Интернете за вами никто не следит? Как бы не так!

Такие компании, как Drawbridge, Tapad и Oracle Crosswise, поднялись на новую ступень в интернет-слежке. Они заявляют, что обладают технологиями, способными отслеживать ваши действия на нескольких устройствах, включая данные, какие сайты вы посещаете исключительно со смартфонов и планшетов.

Частично такая слежка — результат машинного обучения и нечеткой логики. Например, если мобильное устройство и обычный компьютер обращаются к сайту с одного IP-адреса, очень вероятно, что они принадлежат одному человеку. Например, вы произвели поиск какого-то предмета одежды на своем смартфоне, а позже, оказавшись дома и добравшись до обычного компьютера, видите, что этот же предмет одежды отображается на сайте магазина в разделе «недавно просмотренного». Или того лучше, вы покупаете этот предмет одежды, используя компьютер. Чем больше будет совпадений между двумя отдельными устройствами, тем больше вероятность, что ими обоими пользуется один и тот же человек. По заявлению компании Drawbridge, только ей одной удалось связать 1,2 млрд пользователей с 3,6 млрд устройств в 2015 году.

Разумеется, тем же самым занимаются Google, Apple и Microsoft. Смартфоны под управлением операционной системы Android требуют наличия аккаунта Google. Для работы на устройствах Apple необходима учетная запись Apple ID. Не играет роли, смартфон у вас или ноутбук — исходящий трафик каждого будет привязан к конкретному пользователю. А Microsoft в своих последних операционных системах требует создания учетной записи Microsoft, позволяющей скачивать приложения или хранить фотографии и текстовые документы в «облаке» компании.

Огромное различие заключается в том, что в учетных записях Google, Apple и Microsoft можно отключить сбор некоторых или всех данных либо же впоследствии удалить все ранее собранные данные. Компании Drawbridge, Crosswise и Tapad усложняют процесс отключения и удаления. Иногда сделать это просто невозможно.

Хотя с помощью прокси или Tor Browser можно вполне успешно скрывать свое реальное местонахождение при выходе в Интернет, эти манипуляции могут привести к необычным проблемам и трудностям для вас, поскольку иногда сбор интернет-статистики оправдан — например, когда компания, принимающая к оплате банковские карты, пытается выявить подлог. Например, всего за несколько дней до того, как Эдвард Сноуден прославился, он задумал создать сайт по защите прав интернет-пользователей. Но он не сумел расплатиться с хостинговой компанией за регистрацию домена своей банковской картой.

Всего за несколько дней до того, как Эдвард Сноуден прославился, он задумал создать сайт по защите прав интернет-пользователей. Но он не сумел расплатиться с хостинговой компанией за регистрацию домена своей банковской картой.

В то время он еще пользовался своим настоящим именем, настоящим адресом электронной почты и личной банковской картой — дело происходило незадолго до того, как Сноуден превратился в разоблачителя. Также у него был Tor Browser, что иногда заставляет компанию-получателя платежа насторожиться и заподозрить мошенническую операцию. Это происходит, когда компания пытается проверить личность человека, но находит противоречия между предоставленными им сведениями и данными, уже имеющимися у них. Например, если карта была выпущена в Нью-Йорке, почему выходной узел Tor указывает, что вы в Германии? Подобные географические несоответствия часто становятся сигналом о вероятной мошеннической операции, что приводит к дополнительным

проверкам.

Компании, проводящие транзакции по картам, безусловно, следят за нами в Сети. Им известны наши покупки. Они знают, на каких сайтах мы подписаны на платный контент. Они знают, когда мы выезжаем за пределы страны. И они знают, что мы совершаем покупку в Интернете с нового устройства.

Это происходит, когда компания пытается проверить личность человека, но находит противоречия между предоставленными им сведениями и данными, уже имеющимися у них. Например, если карта была выпущена в Нью-Йорке, почему выходной узел Tor указывает, что вы в Германии? Подобные географические несоответствия часто становятся сигналом о вероятной мошеннической операции, что приводит к дополнительным проверкам.

Как утверждает Мика Ли из Фонда электронных рубежей, в какой-то момент Сноуден, находившийся в своем гостиничном номере в Гонконге и обсуждавший государственные тайны с Лорой Пойтрас и Гленном Гринвальдом, репортером издания Guardian, связался со службой поддержки компании DreamHost, хостинг-провайдера из Лос-Анджелеса. Очевидно, Сноуден объяснил компании DreamHost, что находится за границей и не доверяет местным провайдерам Интернета, поэтому выходит в Интернет через Tor. В результате компания DreamHost приняла платеж по банковской карте через Tor.

Один из способов избежать всех этих трудностей с Tor — отредактировать файл geoip/geoip6 так, чтобы этот браузер использовал выходные узлы, расположенные в вашей родной стране. Это должно успокоить компании, принимающие платежи по картам. С другой стороны, один и тот же выходной узел может в итоге способствовать раскрытию вашей личности. Есть основания полагать, что спецслужбы, возможно, контролируют некоторые выходные узлы, поэтому лучше пользоваться разными.

Еще один способ заплатить, не оставляя следов, — оплата биткойнами, виртуальной валютой. Как и большинство валют, она подвержена колебаниям курса, в зависимости от степени доверия к ней.

Еще один способ заплатить, не оставляя следов, — оплата биткойнами, виртуальной валютой.

Биткойн — это алгоритм, с помощью которого пользователь может создавать — или, выражаясь принятыми в этой среде терминами, «майнить» — собственную валюту под названием «биткойн». Однако если бы это было просто, этим бы занимался каждый. Но это не так. Процесс требует высокой вычислительной мощности, на майнинг одного биткойна уходит огромное количество времени. Количество биткойнов ограничено, и это наряду с доверием потребителей влияет на цену одного биткойна.

У каждого биткойна есть криптографическая подпись, удостоверяющая его подлинность и уникальность. Можно отследить все звенья транзакции, осуществляемой с помощью этой криптографической подписи, вплоть до биткойна, однако метод получения этого биткойна можно скрыть — например, создав анонимный электронный ящик, на который вы можете зарегистрировать электронный кошелек для биткойнов, используя сеть Tor.

Вы можете купить биткойны лично или анонимно, оплатив их в Интернете с помощью карты предоплаты. Можно найти банкомат с биткойнами, рядом с которым не установлена камера. В зависимости от того, какие детали могут впоследствии выдать вашу личность, нужно оценить все риски и лишь потом выбирать способ покупки. Далее можно отправить свои биткойны в так называемый миксер. Биткойн-миксер берет несколько биткойнов от меня, несколько биткойнов от вас, несколько — от различных случайных людей и перемешивает их. Вы получаете обратно столько же биткойнов за вычетом платы за услугу, но с другими криптографическими подписями. Благодаря этому достигается некоторая анонимность.

Получив биткойны, как их хранить? Поскольку для биткойнов нет специальных банков, а также поскольку они существуют лишь в виртуальной реальности, вам потребуется анонимно зарегистрированный биткойн-кошелек (подробные инструкции о том, как это сделать, вы найдете далее в этой книге).

Теперь, когда у вас есть биткойны и есть где их хранить, как ими распорядиться? На специальных сайтах-обменниках можно покупать биткойны и менять их на другие валюты, например доллары США, или приобретать на них товары с сайтов типа Amazon. Предположим, что у вас есть один биткойн, стоимость которого на данный момент равна примерно 9 тысячам долларов США. Если вы собираетесь купить что-то, что стоит всего 80 долларов, то после транзакции у вас останется определенная доля от первоначального биткойна (ее величина зависит от текущего курса).

Транзакции верифицируются с помощью открытой базы данных, известной как блокчейн, и идентифицируются посредством IP-адреса. Однако как мы уже видели, IP-адрес можно изменить или подделать. И хотя продавцы начали принимать к оплате биткойны, сервисные сборы, обычно

оплачиваемые продавцами, были возложены на плечи покупателей. Кроме того, в отличие от операций по банковским картам, при оплате биткойнами не бывает возвратов или возмещения средств.

Можно купить столько биткойнов, сколько вы бы купили устойчивой валюты. Но несмотря на свою успешность (братья Уинклвосс, известные судебными тяжбами с Марком Цукербергом из-за социальной сети Facebook, стали главными инвесторами в валюту биткойн), система пережила несколько крупных спадов. В 2004 году токийская биржа криптовалют Mt. Gox объявила себя банкротом, заявив о пропаже всех биткойнов в результате хищения. Были и другие случаи хищения валюты у биткойн-обменников, которые, в отличие от большинства американских банковских счетов, не застрахованы.

Хотя раньше уже предпринимались попытки создать виртуальную валюту, именно биткойн занял место анонимного платежного средства в Интернете. Да, валюта еще развивается, но если вы стремитесь сохранить анонимность, следует рассмотреть этот вариант оплаты.

Возможно, сейчас вы кажетесь себе невидимыми: вы скрыли IP-адрес с помощью Tor, зашифровали электронные письма и текстовые сообщения с помощью программ PGP и Signal. Однако я уделил очень мало внимания аппаратным средствам, с помощью которых можно как найти, так и спрятать вас в Интернете.

Глава 7

ЗАПЛАТИ, А ТО ТЕБЕ НЕ ПОЗДОРОВИТСЯ!

Кошмар начался в Интернете, а завершился вторжением федеральных агентов в один из домов в пригороде Блейна, штат Миннесота. У агентов был только IP-адрес, с которого скачивали детскую порнографию и даже угрожали убийством вице-президенту Джо Байдену. Связавшись с интернет-провайдером, федеральные агенты узнали реальный адрес пользователя. В те дни, когда подключение к Интернету еще было проводным (через модем или маршрутизатор), можно было легко вычислить пользователя таким способом. Тогда по IP-адресу можно было установить точное местонахождение компьютера.

Однако в наше время у большинства людей беспроводное подключение к Интернету. Беспроводное соединение позволяет каждому перемещаться по дому с мобильными устройствами и сохранять подключение. А если вы недостаточно осторожны, то к вашей точке доступа могут подключиться и соседи. В данном случае федеральные агенты ворвались не в тот дом в Миннесоте. На самом деле им нужен был дом по соседству.

Кошмар начался в Интернете, а завершился вторжением федеральных агентов в один из домов в пригороде Блейна, штат Миннесота. У агентов был только IP-адрес, с которого скачивали детскую порнографию и даже угрожали убийством вице-президенту Джо Байдену. Связавшись с интернет-провайдером, федеральные агенты узнали реальный адрес пользователя. В те дни, когда подключение к Интернету еще было проводным (через модем или маршрутизатор), можно было легко вычислить пользователя таким способом. Тогда по IP-адресу можно было установить точное местонахождение компьютера.

В 2010 году Барри Винсент Ардольф был признан виновным в хакерстве, хищении персональной информации, хранении детской порнографии и даже угрозах вице-президенту Джо Байдену. Согласно протоколу судебного заседания, конфликт начался с того, что сосед Ардольфа, который ко всему прочему был еще и юристом (его имя не называется), написал заявление в полицию, обвинив Ардольфа в том, что тот, предположительно, «неподобающим образом трогал и поцеловал» соседского ребенка в губы.

Далее Ардольф подключился к беспроводному домашнему роутеру соседа и зарегистрировал от его имени аккаунты Yahoo! и MySpace. Именно с этих аккаунтов Ардольф запустил кампанию, целью которой было скомпрометировать юриста и вызвать у него проблемы с законом.

Многие интернет-провайдеры теперь по умолчанию встраивают в свои домашние маршрутизаторы возможность беспроводного доступа. Некоторые интернет-провайдеры, например американский Comcast, создают второй, бесплатный Wi-Fi-сервис, которым вы можете управлять лишь отчасти. Например, вы можете изменить некоторые настройки и даже отключить его. Вы должны помнить об этом. В минивэне, припаркованном напротив вашего дома, кто-то бесплатно может пользоваться вашим беспроводным Интернетом. Хотя вам не приходится за это платить дополнительно, скорость соединения может снизиться, если кто-то активно эксплуатирует второй канал. Можно отключить точку доступа (в случае с провайдером Comcast — функцию Xfinity Home Hotspot), если вы считаете, что вам никогда не понадобится раздать Интернет своим гостям.

Хотя встроенная возможность беспроводного подключения — это очень удобно, нередко такие маршрутизаторы настроены не лучшим образом и при отсутствии определенного уровня защиты могут стать источником проблем. Начнем с того, что незащищенный беспроводной доступ может превратиться в цифровую дверь в ваш дом, как и получилось с Ардольфом. Хотя незваных гостей, возможно, не интересуют ваши цифровые документы, они тем не менее могут стремиться навлечь на вас неприятности.

Ардольф не был компьютерным гением. Он признался в суде, что не знает разницы между шифрованием WEP (Wired Equivalent Privacy), которое использовалось роутером соседа, и шифрованием WPA (Wi-Fi Protected Access), которое является гораздо более надежным. Он был просто зол. Именно поэтому необходимо серьезно проанализировать, насколько защищена ваша домашняя беспроводная сеть. Никогда не знаешь, в какой момент обозленный сосед попытается отомстить вам с помощью вашей же домашней сети.

Если кто-то все же пытается навредить вам через ваш домашний маршрутизатор, существуют способы защитить себя. По данным Фонда электронных рубежей (EFF), федеральные судьи отклонили несколько исков правообладателей к пользователям пиринговых сетей, поскольку ответчикам удалось убедить суд в том, что через их точку доступа к Интернету фильмы качал кто-то другой. Фонд электронных рубежей утверждает, что IP-адрес — это не человек, имея в виду, что пользователи беспроводного Интернета не могут отвечать за действия остальных людей, подключившихся к их сети.

Хотя компьютерно-техническая экспертиза установит невиновность домовладельца, чей Wi-Fi стал инструментом в руках преступника — как было в случае с юристом из Миннесоты, — но зачем подвергать себя этому испытанию?

Даже если вы подключаетесь к Интернету через телефонную линию или кабельный маршрутизатор (например, Cisco или Belkin), вы все равно не застрахованы от проблем с программным обеспечением и настройками.

Первое и основное, что необходимо сделать, — скачать новейшую прошивку (программное обеспечение для постоянного запоминающего устройства). Для этого необходимо открыть страницу настроек маршрутизатора (см. ниже) или зайти на сайт производителя и поискать обновления для вашей модели. Чем чаще вы будете это делать, тем лучше. Самый простой способ обновлять прошивку маршрутизатора — каждый год покупать новое устройство. Возможно, это накладно, но так у вас точно будет новейшая и лучшая прошивка. Во-вторых, нужно обновлять настройки маршрутизатора. Не следует довольствоваться настройками по умолчанию.

Самый простой способ обновлять прошивку маршрутизатора — каждый год покупать новое устройство. Возможно, это накладно, но так у вас точно будет новейшая и лучшая прошивка. Во-вторых, нужно обновлять настройки маршрутизатора.

Не следует довольствоваться настройками по умолчанию.

Но сначала разберемся с именем сети: что в нем содержится? Больше, чем может показаться. Маршрутизатор, предоставленный интернет-провайдером, и маршрутизатор, купленный в магазине бытовой электроники, объединяет подход к присвоению имен. Все беспроводные маршрутизаторы по умолчанию транслируют идентификатор SSID (англ. Server Side Identity — «серверный идентификатор»). Обычно SSID включает в себя название и модель маршрутизатора и выглядит, например, следующим образом «Linksys WRT54GL». Если вы посмотрите, как называются беспроводные точки доступа к Интернету в вашем районе, вы поймете, о чем я говорю.

Транслируя предустановленный идентификатор SSID, можно скрыть, из какого именно дома исходит Wi-Fi-сигнал, но при этом любой прохожий будет знать, какая у вас марка и модель маршрутизатора. Что в этом плохого? Этот человек может также быть в курсе, какие уязвимости характерны для данной конкретной модели роутера, и сможет ими воспользоваться.

Так как же изменить название маршрутизатора и обновить прошивку?

Получить доступ к настройкам маршрутизатора просто, это делается через веб-браузер. Если данная информация отсутствует в инструкции к вашему роутеру, в Интернете можно найти сайты, на которых рассказывается, что нужно напечатать в адресной строке браузера, чтобы подключиться напрямую к роутеру. Набрав локальный URL-адрес (помните, что речь идет только о связи с маршрутизатором, а не с Интернетом в целом), вы увидите экран авторизации. Какой логин (имя пользователя) и пароль нужно указать для входа?

Оказывается, в Интернете есть список логинов и паролей, установленных по умолчанию. В данном примере и логином, и паролем для роутера Linksys будет «admin». Стоит ли говорить, что, оказавшись в настройках маршрутизатора, нужно тут же сменить установленный по умолчанию пароль, следуя моим ранее описанным указаниям по созданию уникального и надежного пароля или с помощью менеджера паролей.

Обязательно сохраните новый пароль в своем менеджере паролей или запишите его, поскольку вы вряд ли будете заходить в настройки роутера слишком часто. Если вы вдруг забудете свой пароль (действительно, насколько часто вы собираетесь открывать экран настройки конфигурации маршрутизатора?), не переживайте. На самом устройстве присутствует кнопка сброса, которая позволяет восстановить настройки по умолчанию. Однако после нажатия этой кнопки вам придется заново изменить все параметры, о которых мы будем говорить далее. Поэтому записывайте или распечатывайте снимки экрана со всеми настройками маршрутизатора, которые вы изменили. Эти снимки экрана очень пригодятся, когда вам нужно будет настроить маршрутизатор заново.

Перейдем к настройкам беспроводной сети.

Я предлагаю вам сменить имя SSID «Linksys WRT54GL» на что-то безобидное, например «HP Inkjet», и незнакомец не поймет, из какого дома исходит Wi-Fi-сигнал. Я часто выбираю какое-нибудь непримечательное название, например, название моего жилого комплекса или даже имя соседа.

Также можно вообще скрыть свой SSID. В результате другие не смогут увидеть ваш сигнал в списке беспроводных сетевых соединений.

Пока мы разбираемся с базовыми настройками маршрутизатора, нужно рассмотреть несколько типов защиты беспроводной сети. Обычно настройки защиты по умолчанию отключены. Кроме того, не все виды защиты в равной степени эффективны и не все они поддерживаются каждым

устройством.

Самая базовая форма защиты, протокол шифрования данных в беспроводных сетях WEP (Wireless Encryption

Protocol), бесполезна. Если вы увидите этот пункт в настройках, проигнорируйте его. WEP успешно взламывают уже много лет, поэтому этот протокол рекомендуется не использовать вообще. Данную устаревшую технологию предлагают в качестве защитной меры только старые маршрутизаторы и устройства. Лучше выбрать один из более новых и надежных стандартов шифрования, например WPA (Wi-Fi Protected Access). Протокол WPA2 является еще более надежным.

Когда в настройках маршрутизатора включено шифрование, остальные устройства, подключающиеся к маршрутизатору, должны поддерживать его. Большинство новых устройств автоматически определяют действующий тип шифрования, однако для более старых моделей до сих пор необходимо указывать его вручную. Всегда выбирайте максимально высокий уровень. Вы защищены ровно настолько, насколько защищено ваше самое слабое соединение, поэтому в том, что касается шифрования, из старых устройств выжимайте максимум.

Установите для доступа к своей сети пароль, состоящий не менее чем из 15 символов (цифр и как минимум одной буквы). Или создайте сложный пароль с помощью менеджера паролей.

Настроив WPA2 на маршрутизаторе, вы должны будете настроить его на ноутбуке или мобильном устройстве, хотя некоторые новые операционные системы определяют тип шифрования автоматически. Современная операционная система на смартфоне или ноутбуке определит, что рядом с вами есть точка доступа Wi-Fi. В списке доступных подключений должен будет появиться ваш идентификатор SSID (например, «HP Inkjet»), он будет на самом верху или почти на самом верху. Значки в виде замочка рядом с доступными Wi-Fi-сетями (обычно отображаются над информацией об уровне каждого сигнала) указывают, какие точки доступа Wi-Fi защищены паролем (около вашей точки теперь тоже должен быть замочек).

Из списка доступных сетей выберите SSID своей беспроводной сети. После этого необходимо будет ввести пароль, состоящий как минимум из 15 символов, установленный ранее. Чтобы подключиться к защищенному паролем Wi-Fi-соединению, нужно ввести свой пароль на каждом устройстве хотя бы один раз, поэтому менеджер паролей в некоторых случаях не подходит, в частности если вам нужно запоминать сложный пароль, чтобы позже вводить его самостоятельно. На каждом устройстве, которое вы захотите подключить к своей сети, включая «умный» холодильник и цифровой телевизор, нужно ввести пароль и выбрать тот тип шифрования, который установлен в настройках маршрутизатора. Это необходимо сделать при первом подключении каждого отдельного устройства к домашней или рабочей сети Wi-Fi, но далее вы будете избавлены от этой необходимости, пока не смените пароль или не купите новое устройство.

Можно пойти дальше и ограничить количество возможных подключений к своей точке доступа Wi-Fi, определив разрешенные устройства. Это так называемый белый список, или фильтрация по MAC-адресам. Вы разрешаете доступ определенным устройствам (белый список) и запрещаете всем остальным (черный список). Для этого необходимо добавить в белый список MAC-адрес своего устройства (от англ. Media Access Control — «управление доступом к среде»). При этом, когда вы купите очередной смартфон, вам также необходимо будет внести его MAC-адрес в белый список своего маршрутизатора, чтобы он смог подключиться к сети. Этот адрес уникален для каждого устройства. В сущности, первые восемь цифр адреса — это код производителя, а последние четыре уникальны для каждого устройства. Маршрутизатор отклонит любое устройство, MAC-адрес которого не был добавлен в список фильтрации.

Важно отметить, что хакерский инструмент под названием aircrack-ng позволяет узнать авторизованный MAC-адрес подключенного к сети устройства, а затем хакер может сфальсифицировать этот MAC-адрес, чтобы подключиться к данному маршрутизатору. Фильтрация MAC-адресов не стопроцентная гарантия от несанкционированных подключений к вашей сети, как и сокрытие идентификатора SSID.

Узнать MAC-адрес своего устройства довольно просто: в операционной системе Windows нажмите кнопку **Пуск** (Start), напечатайте **cmd**, выберите пункт **Командная строка** (Command promt) и в открывшемся окне оболочки командной строки введите команду **getmac /v /fo list**. Нажмите клавишу **Enter**. Вы увидите длинный список данных, но среди них должен быть MAC-адрес (указан в строке **Физический адрес** (Physical Address) в сводке по вашему сетевому адаптеру). Он состоит из двенадцати символов (букв и цифр), через каждые два символа стоит двоеточие. Если у вас устройство Apple, то все еще проще: раскройте меню  , выберите пункт **Системные настройки** (System preferences) и щелкните мышью по значку **Сеть** (Network). Затем выберите свой сетевой адаптер в левой части окна и нажмите кнопку **Дополнительно** (Advanced), и на вкладке аппаратных средств вы увидите MAC-адрес. На более старых компьютерах Mac процесс аналогичен, только в разделе **Сеть** (Network) окна **Системные настройки** (System preferences) нужно выбрать пункт **Встроенный Ethernet** (Built-in Ethernet).

Чтобы определить MAC-адрес смартфона, на устройстве iPhone/iPad коснитесь значка **Настройки** (Settings) и выберите пункт **Основные —> Об этом устройстве** (General — > About), и взгляните на значение в строке **Адрес Wi-Fi** (Wi-Fi Address).

На устойстве Android также коснитесь значка **Настройки** (Settings) и выберите пункт **О телефоне —> Общая информация** (About Phone —> Status), и взгляните на значение в строке **MAC-адрес Wi-Fi** (Wi-Fi MAC address). Доступ к нужной информации может быть иным в зависимости от типа и модели устройства.

Зная двенадцатизначные MAC-адреса, можно настроить маршрутизатор так, чтобы он предоставлял доступ к сети только этим устройствам и блокировал все другие. Тут есть несколько слабых моментов. Если к вам придет гость и захочет подключиться к домашней сети, вам придется выбирать, дать ли этому человеку одно из своих устройств и пароль от него или просто открыть настройки конфигурации маршрутизатора и отключить фильтрацию по MAC-адресам. Иногда MAC-адрес устройства приходится изменить, и, если потом не вернуть его обратно, вы не сможете подключиться к своей домашней или рабочей сети Wi-Fi с настроенной фильтрацией по MAC-адресам. К счастью, в большинстве случаев, чтобы вернуть исходный MAC-адрес, достаточно просто перезагрузить устройство.

Чтобы можно было без труда подключать любое новое устройство к домашнему маршрутизатору, альянс совместимости беспроводного оборудования (Wi-Fi Alliance), занимающийся распространением Wi-Fi-технологий, разработал протокол WPS (от англ. Wireless Protected Setup — «защищенная настройка беспроводного соединения»). WPS позиционировался как протокол, с помощью которого любой человек — действительно кто угодно — сможет быстро и безопасно подключить свои мобильные устройства к домашней или рабочей сети. Но в реальности уровень безопасности оказался не таким уж высоким.

WPS обычно реализован в виде кнопки на роутере. Также он может быть представлен в виде кода, передаваемого посредством технологии NFC (от англ. Near Field Communication — «ближняя бесконтактная связь»). Простыми словами, вы активируете функцию WPS, и протокол связывается с каждым устройством в вашем доме или офисе и автоматически синхронизирует их с вашей Wi-Fi-сетью.

Звучит отлично. Однако если маршрутизатор находится в доступном месте, например в гостиной, любой человек может нажать кнопку WPS и подключиться к вашей домашней сети.

Даже не имея возможности нажать кнопку, злоумышленник может взломать PIN-код WPS методом перебора. У него на это может уйти четыре часа, но такое может произойти, поэтому необходимо защитить себя, немедленно отключив функцию WPS на роутере.

Еще один метод взлома WPS называется «PixieDust». Это оффлайновый метод взлома, который применим только к устройствам с микросхемами определенных производителей, включая Ralink, Realtek и Broadcom. PixieDust позволяет хакеру получить пароли к беспроводному маршрутизатору. В целом, инструмент действует очень целенаправленно и позволяет подобрать пароль к устройству за несколько секунд или часов, в зависимости от сложности выбранного или сгенерированного PIN-кода. Например, одна из таких программ под названием Reaver позволяет взломать маршрутизатор с WPS в течение нескольких часов.

Подводя итог, лучше отключить WPS. Можно просто вручную подключать каждое новое мобильное устройство к своей сети, вводя установленный ранее пароль.

Итак, с помощью шифрования и надежных паролей вы предотвратили несанкционированное подключение к вашему беспроводному маршрутизатору посторонних людей. Означает ли это, что никто не сумеет проникнуть в вашу домашнюю сеть или даже виртуально попасть в ваш дом? Не совсем.

Когда старшеклассника Блейка Роббинса вызвали на беседу к директору школы в пригороде Филадельфии, он понятия не имел, что его ждет выговор за «неподобающее поведение» у себя дома. Школьный округ Нижнего Мериона в предместьях Филадельфии выдал всем своим старшеклассникам, включая Роббинса, новые ноутбуки MacBook для учебы. Однако администрация школы не сообщила ученикам, что программное обеспечение, предназначенное для поиска устройства в случае его потери, также могло применяться для слежки за всеми 2300 школьниками, пока те находились в зоне видимости веб-камеры компьютера.

В чем обвинили Роббинса? В том, что он глотал таблетки. Семья Роббинса с помощью адвоката отстаивала утверждение, что школьник, делая уроки, ел обычные конфетки Mike and Ike.

Почему вообще возникла эта проблема?

Школьный округ настаивает, что программа Theft Track была активирована лишь после кражи одного из ноутбуков. Программа Theft Track действует следующим образом: когда пользователь

программы заявляет о пропаже ноутбука, школа может войти в учетную запись на сайте и посмотреть фотографии, сделанные веб-камерой ноутбука, а также прослушать звук с микрофона. Школьный администратор должен отследить ноутбук и при необходимости сделать снимки. Так можно найти устройство и вернуть его пользователю, а также вычислить виновного. Однако в данном случае школьную администрацию обвинили в том, что с помощью этой функции осуществлялась слежка за школьниками у них дома.

Веб-камера на полученном от школы ноутбуке Роббинса сделала сотни снимков, на некоторых из которых мальчик спит в кровати. Ситуация других школьников была еще хуже. Согласно свидетельским показаниям в суде, у школы были даже фотографии учеников в «частично оголенном» виде. Все это могло бы остаться незамеченным, если бы Роббинса не обвинили в тех вещах, которыми он, предположительно, занимался только дома.

Роббинс вместе с бывшим учеником Джалилом Хасаном, на которого у школы было досье из примерно 500 снимков его самого и 400 снимков экрана его компьютера (снимки посещенных им сайтов), подал иск против школьного округа. Роббинс получил компенсацию размером 175 000 долларов США, а Хасан — 10 000 долларов. Кроме того, с округа взыскали примерно полмиллиона долларов за судебные издержки детей. В итоге школьный округ через свою страховую компанию выплатил около 1,4 миллиона долларов.

Вредоносное программное обеспечение может без труда включить камеру и микрофон на компьютере человека, а тот даже не будет об этом догадываться. И то же самое с мобильным устройством. В данном случае это было спланированное и продуманное действие. Но очень часто это не так. Быстрый способ обезопасить себя — заклеить камеру ноутбука непрозрачным скотчем на то время, пока вы ей не пользуетесь.

Осенью 2014 года Софи Кертис, журналистка лондонского издания Telegraph, получила электронный запрос с портала LinkedIn, который будто бы исходил от ее коллеги по газете. Софи часто получала подобные письма и, руководствуясь профессиональной солидарностью, без колебаний принимала такие запросы от коллег. Через несколько недель она вдруг получила электронное письмо якобы от группы анонимных разоблачителей, которые собирались обнародовать некие секретные документы. Будучи журналисткой, интересовавшейся деятельностью таких организаций, как Anonymous и WikiLeaks, она неоднократно получала подобные письма. И она заинтересовалась. Вложенный файл казался обычным, и Софи открыла его.

Журналистка тут же поняла, что что-то пошло не так. Windows Defender, антивирусная программа, встроенная в операционную систему Windows, начала выдавать предупреждения, которых с каждой секундой становилось все больше.

Кертис, как и многих в наше время, обманом убедили нажать на вложение, которое, как ей казалось, было обычным файлом. Создав впечатление, что он содержит интересующую ее информацию, файл на самом деле загрузил и распаковал ряд других файлов, с помощью которых хакеры взяли под свой полный контроль ее компьютер. Вредоносная программа даже сфотографировала женщину с помощью ее же веб-камеры. На этом снимке Софи выглядит совершенно обескураженной, пытаясь понять, как кому-то удалось влезть в ее компьютер.

На самом деле журналистке было прекрасно известно, кто захватил компьютер. За несколько месяцев до этого она ради интереса наняла тестировщика на уязвимости, или пентестера. Кого-то вроде меня. Компании и частные лица нанимают профессиональных хакеров, чтобы те попытались взломать их компьютер или компьютерную сеть. Так можно понять, где нужно усилить защиту. В случае с Кертис проверка растянулась на несколько месяцев.

Приступая к подобной работе, я всегда стараюсь узнать о клиенте как можно больше. Я много времени трачу на то, чтобы узнать, как он живет и чем занимается в Интернете, слежу за постами на ресурсах Twitter, Facebook и, да, даже LinkedIn. Именно это и сделал специалист, нанятый Софи Кертис. Среди электронных писем женщины оказалось одно тщательно сконструированное послание от пентестера — первое письмо. Он знал, что она журналистка и что она с легкостью принимает запросы от незнакомых людей. Касательно первого письма Кертис позже написала, что там было недостаточно информации, чтобы заинтересовать ее и вызвать у нее желание провести интервью и написать статью о том человеке. Но ее впечатлил масштаб исследовательской работы, проделанной хакером и его коллегами.

Кертис сказала: «Они сумели с помощью Twitter узнать мой рабочий электронный ящик, а также несколько мест, где я недавно побывала, и название общественного мероприятия, которое я регулярно посещаю вместе с другими журналистами. По вещам на заднем плане одной из выложенных мной в Twitter фотографий им удалось выяснить, какой у меня был мобильный телефон, а также что мой жених раньше курил самокрутки (это была старая фотография) и что он увлекается велосипедным спортом». Любой из этих деталей хватило бы для того, чтобы составить такое письмо.

Также на конференции DEF C0N2016 был анонсирован новый инструмент на базе искусственного интеллекта. С помощью этого инструмента можно будет анализировать твиты жертвы. После этого инструмент сможет составить фишинговое письмо, ориентируясь на интересы человека. Поэтому будьте осторожны, переходя по ссылке из твита.

И правда, часто самые незначительные мелочи — лишний комментарий, оставленный тут или там, необычная побрякушка на полке за вашей спиной на фотографии, футболка с логотипом летнего лагеря, где вы побывали — становятся дополнительным источником важнейшей личной информации, которой вы вовсе не собирались ни с кем делиться. Нам может казаться, что эти не связанные между собой детали безобидны, но чем больше подробностей выяснит злоумышленник, тем легче ему будет убедить вас открыть прикрепленный к письму файл и захватить контроль над вашим цифровым миром.

Кертис отметила, что тестировщики на этом остановились. Будь они настоящими преступниками, процесс мог бы продолжаться еще какое-то время. Возможно, хакеры взломали бы ее аккаунты в соцсетях, рабочую сеть издания Telegraph и даже проникли бы в банковский счет. И вероятнее всего, они бы сделали это таким образом, что Кертис даже не поняла бы, что ее компьютер был взломан, — большинство атак не провоцируют реакцию Windows Defender или другого антивируса. Некоторые хакеры проникают в компьютер и затихают, а пользователь может не догадываться об этом многие месяцы и даже годы. Это касается не только ноутбука, но и перепрошитого iPhone (т. е. с джейлбрейком) или мобильного устройства на операционной системе Android.

Хотя Google и другие сервисы электронной почты проверяют ваши письма на предмет вредоносного программного обеспечения и порнографического контента, а также для получения статистических данных в рекламных целях, но они не ставят своей целью защитить вас от мошеннических схем. Как и с конфиденциальностью, которую, как мы уже говорили, каждый понимает по-своему, с мошенничеством дела обстоят трудно. Мы не всегда можем его распознать, даже когда оно у нас прямо под носом.

В полученном Кертис фальшивом письме с LinkedIn содержалось однопиксельное изображение, неприметная точка, как те, с помощью которых некоторые веб-сайты следят за своими посетителями (мы говорили об этом ранее). Когда эта крошечная точка отвечает на запрос, она передает занимающемуся сбором данных серверу, который может быть расположен в любой точке мира, информацию о том, когда, на какое время и с какого устройства вы открывали это письмо. Также программный код сообщает, было ли письмо сохранено, перенаправлено или удалено. Кроме того, если бы атака была настоящей, хакеры могли бы добавить в письмо ссылку на фальшивую страницу LinkedIn, которая бы в точности имитировала настоящую страницу с тем лишь исключением, что размещалась бы на другом сервере, возможно, вообще в другой стране.

Хотя Google и другие сервисы электронной почты проверяют ваши письма на предмет вредоносного программного обеспечения и порнографического контента, а также для получения статистических данных в рекламных целях, но они не ставят своей целью защитить вас от мошеннических схем.

Для рекламодателя эта брешь в системе безопасности — отличная возможность для сбора данных о получателе (и составления его профиля). Для хакеров это

способ выяснить технические характеристики, необходимые для разработки плана перехвата контроля над вашей машиной. Например, если вы используете устаревшую версию браузера, там могут быть уязвимости, которые сыграют хакерам на руку.

Второе письмо, полученное Кертис от тестировщиков, содержало вложение, электронный документ, использующий уязвимости программы, с помощью которой он открывался (допустим, Adobe Reader). Когда мы говорим о вредоносных программах, большинство людей вспоминает компьютерные вирусы начала 2000-х, когда одно зараженное электронное письмо распространяло копии зараженных писем всем адресатам из списка контактов. Подобные массовые атаки в наше время случаются гораздо реже, отчасти потому что изменились сами почтовые программы. Напротив, современные вредоносные программы действуют гораздо более тонко и часто подстраиваются под конкретного человека. Именно так и было в случае с Софи Кертис. Тестировщики применили особый вид фишинга, известный как направленный фишинг, целью которого является конкретный человек.

Фишинг — это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным человека, таким как логины, пароли, данные банковских карт или финансовая информация. Распространенная фишинговая схема заключается в том, что хакер обманом убеждает финансового директора перевести крупную сумму денег под тем предлогом, что якобы так распорядился генеральный директор. Обычно в фишинговом письме или сообщении содержится активный элемент, например, кликабельная ссылка или открывающееся вложение. Что же касается Кертис, хакеры внедрили вредоносную программу на ее компьютер, просто чтобы показать, насколько это легко.

Среди наиболее известных фишинговых атак была «Операция Аврора», когда получателями фишингового письма были китайские сотрудники Google. Злоумышленники хотели заразить вирусом компьютеры компании в Китае, чтобы получить доступ к внутренней сети главного представительства Google в Маунтин-Вью, Калифорния. Хакерам это удалось, они очень близко подобрались к исходному коду поисковой системы Google. Пострадал не только Google. Другие компании, например Adobe, жаловались на аналогичные атаки. В итоге компания Google быстро свернула свою деятельность на территории Китая.

Каждый раз, когда мы получаем запрос с сайта LinkedIn или Facebook, наша защита потенциально ослабевает. Вероятно, потому что мы доверяем этим сайтам и автоматически доверяем электронным письмам от них. Но как мы видели, кто угодно может подделать сообщение, и оно будет выглядеть правдоподобно. При живом общении мы обычно видим, что у собеседника накладные усы или шиньон или же что он пытается изменить голос. Сотни лет эволюции развили наши инстинкты настолько, что мы подсознательно улавливаем ложь. Эти инстинкты не действуют в Интернете, по крайней мере, у большинства из нас. Софи Кертис была журналисткой, по роду деятельности ей положено быть любопытной и недоверчивой, ведь она должна распутывать клубки событий и проверять факты. Софи могла бы проверить наличие пользователя LinkedIn в списке сотрудников издания Telegraph. Тогда бы она поняла, что письмо, вероятно, фальшивка. Но она так не сделала. И в обычной жизни многие из нас так же беспечны.

У хакера, который занимается фишингом, будет какая-то информация о вас, но не вся. Тот маленький кусочек ваших персональных данных, который есть у мошенника, он будет использовать как наживку. Например, злоумышленник может отправить вам письмо, содержащее последние четыре цифры вашей банковской карты, чтобы вы начали ему доверять, а затем он начнет выпытывать у вас другие сведения. Иногда последние четыре цифры карты неверны, и мошенники в ответ попросят вас поправить их. Не делайте этого. Если кратко, не вступайте ни в какое взаимодействие с мошенником. Не отвечайте на запросы персональной информации, даже если они кажутся вам добросовестными. Наоборот, свяжитесь с указанной организацией с отдельного электронного ящика (если у вас есть ее адрес) или напишите текстовое сообщение (если известен номер мобильного телефона).

Наибольшую опасность представляют те фишинговые атаки, которые обманом заставляют жертву выполнить то действие, в результате которого хакер получает полный контроль над компьютером. Именно этого я пытаюсь достичь путем социальной инженерии. Также распространен такой тип атаки, при котором злоумышленник выведывает логин и пароль жертвы, но настоящая опасность целевого фишинга связана с получением доступа к компьютеру и сети жертвы.

Что делать, если вы все-таки ответили мошеннику и в результате потеряли все свои материалы — личные фотографии, конфиденциальные документы — с зараженного компьютера или мобильного устройства? Именно это и произошло с матерью Алины Симон. Журналистка New York Times Симон описала, как ее мама — не отличавшаяся особой компьютерной грамотностью — столкнулась с хитроумным врагом в лице вируса-вымогателя.

В 2014 году Интернет накрыла волна вирусов-вымогателей, жертвами которых становились как частные лица, так и корпорации. Одна из таких программ называется Cryptowall. Она шифрует все содержимое вашего жесткого диска, блокируя пользователю доступ ко всем файлам, пока он не заплатит хакеру за ключ для разблокировки.

Если у человека нет резервных копий содержимого компьютера или мобильного устройства, он не увидит своих файлов, пока не заплатит вымогателям.

В 2014 году Интернет накрыла волна вирусов-вымогателей, жертвами которых становились как частные лица, так и корпорации. Одна из таких программ называется Cryptowall. Она шифрует все содержимое вашего жесткого диска, блокируя пользователю доступ ко всем файлам, пока он не заплатит хакеру за ключ для разблокировки. Если у человека нет резервных копий содержимого компьютера или мобильного устройства, он не увидит своих файлов, пока не заплатит вымогателям.

Не хотите платить? В появляющемся на экране сообщении от вымогателей говорится, что ключ для разблокировки файлов будет уничтожен в течение определенного промежутка времени. Часто это послание сопровождается часами с обратным отсчетом, но иногда, если вы не платите, крайний срок откладывается, хотя с каждой такой отсрочкой возрастает цена.

В целом, лучше не нажимать на вложения (хотя вы можете просмотреть их, используя функцию Google Быстрый просмотр или сервис Google Документы). И все же программа Cryptowall может распространяться и иначе. Например, через рекламные баннеры на веб-сайтах. Просто зайдя на страницу с зараженным баннером, можно занести вирус на свой компьютер — это называется «скрытая загрузка», потому что вы на самом деле не нажимаете на рекламу. Это именно тот случай, когда расширения для блокировки рекламы, такие как Adblock Plus, сослужат вам хорошую службу.

За первые шесть месяцев 2015 года входящий в структуру ФБР Центр по приему жалоб на мошенничество в Интернете (Internet Crime Complaint Center, IC3) зафиксировал около тысячи случаев заражения вирусом Cyptowall 3.0, а нанесенный ущерб составил около 18 миллионов долларов. Эта сумма включает в себя размер выплаченных выкупов, стоимость услуг IT-специалистов и ремонтных мастерских, а также потери рабочего времени. В некоторых случаях зашифрованные файлы содержали весьма важные персональные данные (например, номер социального страхования), что подпадает под определение утечки данных и влечет за собой еще большие расходы.

Хотя ключ дешифровки всегда можно приобрести за сумму от 500 до 1000 долларов, обычно жертвы атаки пытаются решить проблему иначе — например, самостоятельно взломать шифр, чтобы избавиться от вируса-вымогателя. Именно так и попыталась поступить мама Симон. Когда она наконец позвонила своей дочери, время было почти на исходе.

Почти каждый, кто когда-либо пытался самостоятельно дешифровать данные, захваченные вирусом-вредителем, потерпел фиаско.

Почти каждый, кто когда-либо пытался самостоятельно дешифровать данные, захваченные вирусом-вредителем, потерпел фиаско. Шифрование очень мощное, и для его взлома требуются более мощные компьютеры и больше времени, чем доступно большинству людей. Поэтому обычно жертвы платят. По словам Симон, офис шерифа округа Диксон в Теннесси в 2014 году заплатил выкуп вымогателям, чтобы те разблокировали отчеты о вскрытии, свидетельские показания, фотографии с мест преступления и другие документы (количеством 72 000 единиц), зашифрованные с помощью программы Cryptowall.

Часто хакеры требуют оплаты в биткойнах, а следовательно, большинству людей трудно заплатить. Биткойн, как я уже говорил, представляет собой децентрализованную пиринговую цифровую валюту, и у большинства людей нет биткойн-кошельков, с которых они могли бы снять средства.

В своей статье в Times Симон напоминает читателям, что нельзя платить вымогателям — и все же именно это она в итоге и сделала. На самом деле сейчас ФБР советует в таких случаях просто заплатить. Джозеф Бонаволонта, заместитель руководителя бостонского подразделения ФБР по борьбе с киберпреступностью, заявил: «Честно говоря, мы часто рекомендуем людям просто заплатить выкуп». По его словам, даже ФБР не в состоянии взломать шифр, применяемый авторами программ-вымогателей. Бонаволонта добавил, что хотя за прошлые годы множество людей заплатило выкуп, цена в 500 долларов остается практически неизменной. Позже ФБР заявило, что компании должны сами решать, платить ли им выкуп или обращаться к другим специалистам по безопасности.

Мама Симон, которая за всю свою жизнь не купила ни одного приложения, позвонила дочери на одиннадцатом часу срока, чтобы узнать, как произвести оплату в цифровой валюте. Симон нашла на Манхэттене банкомат для биткойнов, с помощью которого она (столкнувшись с программным сбоем и позвонив в службу поддержки) в конце концов совершила платеж. В тот день один биткойн стоил чуть более 500 долларов.

Независимо от того, получают ли вымогатели выкуп наличными или в биткойнах, они остаются анонимными, хотя существуют технические возможности отследить оба вида платежей. По транзакциям, проводимым в сети через биткойны, можно вычислить покупателя — хоть это и непросто. Вопрос в том, кто станет тратить время и силы на поиск этих преступников?

Сейчас ФБР советует в таких случаях просто заплатить. Джозеф Бонаволонта, заместитель руководителя бостонского подразделения ФБР по борьбе с киберпреступностью, заявил: «Честно говоря, мы часто рекомендуем людям просто заплатить выкуп».

В следующей главе я расскажу, что может произойти, если вы выйдете в Интернет через публичную точку доступа Wi-Fi. С точки зрения информационной безопасности, Wi-Fi в общественных местах обеспечивает желанную анонимность, но необходимо также соблюдать меры предосторожности.

Глава 8

ВСЕМУ ВЕРЬ, НИЧЕМУ НЕ ДОВЕРЯЙ

Когда телефоны еще были техническим новшеством, они были физически вмонтированы в стену дома, иногда даже в специальную нишу. Наличие второй линии считалось роскошью. Кроме того, в общественных местах раньше были оборудованы телефонные будки, чтобы можно было поговорить без свидетелей. Даже таксофоны в холлах отелей были разделены звукопоглощающими перегородками, чтобы создать иллюзию приватности.

С появлением мобильных телефонов это ощущение приватности совершенно стерлось. Проходя по улице, нередко можно услышать, как люди громко обсуждают свои личные дела или — и того хуже — диктуют реквизиты своего банковского счета. На фоне сформировавшейся культуры открытости и публичности мы должны ясно осознавать, какой информацией делимся с миром.

Иногда мир вас внимательно слушает. Просто задумайтесь.

Проходя по улице, нередко можно услышать, как люди громко обсуждают свои личные дела или — и того хуже — диктуют реквизиты своего банковского счета. На фоне сформировавшейся культуры открытости и публичности мы должны ясно осознавать, какой информацией делимся с миром.

Иногда мир вас внимательно слушает.

Просто задумайтесь.

Допустим, вам нравится работать в кафе за углом вашего дома, как мне. Там бесплатный Wi-Fi. Кажется, что это неплохо, да? Не хочется вас огорчать, но нет. Общественный Wi-Fi создавался не для интернет-банкинга или электронных платежей. Такой доступ в Интернет невероятно удобен и ровно в такой же степени уязвим. Не вся эта уязвимость имеет техническую природу. Отчасти источником этой уязвимости являетесь вы сами, и хочется верить, можете перестать им быть.

Как понять, что вы подключились к публичной сети Wi-Fi? Очень просто: для выхода в Интернет вам не придется вводить пароль. Чтобы продемонстрировать, насколько вы уязвимы при подключении к публичной сети Wi-Fi, специалисты из компании F-Secure (разработчика антивирусных программ) создали собственную точку доступа. Эксперимент проводился в двух разных популярных общественных местах в центре Лондона — в кафе и публичном пространстве. Результаты их потрясли.

В первом эксперименте исследователи организовали точку доступа в одном из кафе в оживленной части Лондона. Когда постоянные посетители выбирали, к какой сети подключиться, сигнал F-Secure был одновременно и сильным, и бесплатным. Кроме того, в браузере пользователя появлялся баннер с условиями пользовательского соглашения. Возможно, вы встречали подобные баннеры в своей ближайшей кофейне — там рассказывается, что можно и что нельзя делать, пользуясь предоставляемым сервисом. В данном эксперименте условия использования этой бесплатной сети предполагали передачу владельцам сервиса своего первенца или домашнего питомца. Эти условия приняли шесть человек. По правде говоря, большинство людей не тратят время на чтение того, что написано мелким шрифтом, — они просто торопятся перейти к использованию сервиса. И все же нужно хотя бы бегло их просматривать. В данном случае компания F-Secure заявила, что ни она, ни ее юристы не собираются ничего делать с детьми и домашними животными пользователей.

Главной проблемой становится то, что информация, в этой сети будет видна посторонним. В вашей домашней беспроводной сети используется WPA2-шифрование. Это значит, что, если кто-то за вами следит, он не увидит, чем вы занимаетесь в Интернете. Он увидит только, какие сайты вы посещаете. Но бесплатная общественная сеть Wi-Fi в кофейне или аэропорту выставляет исходящий трафик на всеобщее обозрение.

Опять же вы можете спросить, и что такого? Прежде всего вы не знаете, кто за вами наблюдает. В нашем случае это была команда специалистов из компании F-Secure, которая по этическим соображениям удалила все собранные данные, но окажись на их месте преступники, вряд ли они поступили бы так же. Они бы продали данные о вашей электронной почте спамерам, или попробовали бы продать вам что-нибудь, или вообще заразили бы компьютер и мобильное устройство вирусом. И даже могли бы задействовать информацию, полученную из вашей незашифрованной электронной переписки, в целевом фишинге.

Во втором эксперименте исследовательская группа организовала точку доступа на балконе в непосредственной близости от здания британского парламента, штаб-квартиры Лейбористской и Консервативной партий и Национального криминального агентства Великобритании. В течение 30 минут к экспериментальной бесплатной точке доступа подключилось 250 человек. В большинстве случаев устройство подключалось к точке доступа автоматически. Иначе говоря, пользователь не сам выбирал сеть, за него это делало устройство.

Здесь нужно пояснить пару моментов. Давайте сначала разберемся, как и почему мобильное устройство автоматически подключается к сети Wi-Fi.

Ваш компьютер и все мобильные устройства запоминают точки доступа Wi-Fi, как публичные, так и частные, к которым вы подключались. Это хорошо, потому что вы избавлены от необходимости постоянно проходить идентификацию при каждом подключении к излюбленной сети Wi-Fi — например, у себя дома или на работе. Но есть и отрицательная сторона. Если вы заходите в новое кафе, в котором никогда раньше не бывали, вы можете вдруг случайно обнаружить, что уже подключены к Интернету. Что в этом плохого? А то, что, возможно, это интернет-соединение не имеет никакого отношения к данному кафе.

Если вы заходите в новое кафе, в котором никогда раньше не бывали, вы можете вдруг случайно обнаружить, что уже подключены к Интернету. Что в этом плохого? А то, что, возможно, это интернет-соединение не имеет никакого отношения к данному кафе.

Может получиться так, что мобильное устройство поймало сигнал, совпавший с профилем одного из ваших недавний интернет-соединений. Возможно, у вас мелькнет мысль, что что-то здесь не так — слишком уж быстро вы подключились к Интернету в совершенно новом для себя месте, — но в этот момент вы уже будете с головой погружены в какой-нибудь шутер от первого лица и не захотите размышлять на эту тему.

Как в таких случаях происходит автоматическое подключение к Wi-Fi сети? Как я объяснил в предыдущей главе, возможно, дома вам Интернет предоставляет провайдер Comcast, в этом случае у вас дома функционирует бесплатное, незашифрованное интернет-соединение, идентификатор сети (SSID) которого выглядит как «xfinity» и которое входит в пакет услуг. Устройство с Wi-Fi-адаптером могло подключиться к этой сети когда-то раньше. Но как убедиться, что именно так и обстоят дела? А вдруг тот сидящий за угловым столиком парень с ноутбуком раздает бесплатный Интернет с фальшивым SSID «xfinity»?

Предположим, что вы в самом деле подключились к точке доступа того странного парня в углу, а не к сети, принадлежащей кафе. Во-первых, вы даже в этом случае сможете путешествовать по Интернету. Вы сможете продолжать играть в любимую игру. Однако каждый пакет данных, который вы отправляете и получаете через Интернет, будет виден этой темной личности с фальшивой точкой доступа к беспроводной сети.

Если он потрудился и создал фальшивую точку доступа к Интернету, значит, вероятно, он перехватывает эти пакеты с помощью бесплатного приложения наподобие WireShark. Я часто работаю с этим приложением, когда занимаюсь поиском уязвимостей. Так я могу посмотреть, что происходит в ближайшей ко мне сети. Я вижу IP-адреса сайтов, на которые заходят пользователи, и сколько времени они проводят на этих сайтах. Если соединение не зашифровано, в перехвате трафика нет ничего противозаконного, поскольку эта информация открыта для всех. Например, будучи системным администратором, мне бы хотелось знать, чем занимаются в моей сети.

Возможно, мутный парень в углу просто шпионит, но никак не влияет на трафик. Но он может влиять на него, причем с несколькими целями.

Может быть, он перенаправляет ваши пакеты данных на прокси-сервер, который устанавливает в ваш браузер программный код JavaScript для клавиатурного шпионажа, чтобы перехватить ваши данные, когда вы зайдете на сайт Amazon. Возможно, ему платят за то, чтобы он выведал ваши идентификационные данные — логин и пароль. Помните, что к учетным записям на сайтах типа Amazon привязана ваша банковская карта.

В своих презентациях Keynote я демонстрирую, как можно перехватить идентификационные данные жертвы, как только она подключилась к моей точке доступа. Поскольку я являюсь промежуточным звеном между вами и сайтом, которому вы пытаетесь отправить запрос, я также могу добавить сценарий JavaScript, который будет загружать фальшивые обновления продуктов Adobe, и в случае их запуска они заразят устройство вирусами. Обычно цель этих атак заключается в том, чтобы заставить вас ввести свой логин и пароль, а затем украсть ваши персональные данные.

Когда человек за угловым столиком совершает махинации с интернет-трафиком, это называется атакой посредника, или атакой «человек посередине» (англ. Man-in-the-Middle). Хакер перенаправляет ваши пакеты данных на настоящий сайт, но при этом перехватывает трафик или изменяет его.

Зная, что вы можете по ошибке подключиться к сомнительной точке доступа Wi-Fi, как это можно предотвратить? Если вы пользуетесь ноутбуком, он обычно выполняет поиск предпочтительной беспроводной сети, а затем подключается к ней. Однако некоторые ноутбуки и мобильные устройства выбирают сеть автоматически. Это задумано с тем, чтобы вам было максимально удобно переносить свое устройство от одной точки к другой. Но как я говорил, у этой медали есть и обратная сторона.

Как утверждает компания Apple, ее устройства автоматически подключаются к сетям в следующем порядке приоритета:

1. Защищенная сеть, к которой устройство подключалось в последний раз.

2. Другая защищенная сеть.

3. Публичная незащищенная сеть.

К счастью, ноутбуки позволяют удалять данные беспроводных соединений, которые больше не нужны — например, той Wi-Fi-сети, к которой вы подключались прошлым летом в отеле, когда были в командировке. В операционной системе Windows (на ноутбуке) можно сбросить флажок **Подключаться автоматически** (Connect Automatically), который отображается рядом с именем беспроводной точки доступа до тех пор, пока вы не подключитесь. Или откройте окно **Панель управления** (Control panel) и щелкните мышью по пункту **Центр управления сетями и общим доступом** (Network and Sharing Center). Щелкните мышью по названию-ссылке подключенной сети и в открывшемся окне нажмите кнопку **Свойства беспроводной сети** (Wireless Properties). Сбросьте флажок **Подключаться автоматически, если есть в радиусе действия** (Connect automatically when this network is in range).

В операционной системе macOS запустите приложение **Системные настройки** (System Preferences) и щелкните мышью по пункту **Сеть** (Network). Выберите пункт **Wi-Fi** и нажмите кнопку **Дополнительно** (Advanced). Затем сбросьте флажок **Запоминать сети, к которым подключается компьютер** (Remember networks this computer has joined). Также можно «забыть» определенную сеть, выбрав ее в списке и нажав кнопку в виде знака минус в нижней части окна.

На устройствах под управлением операционной системы Android и iOS также можно удалять ранее использовавшиеся Wi-Fi-соединения. Если у вас iPhone, iPad или iPod, откройте экран **Настройки** (Settings), выберите раздел **Wi-Fi**. Коснитесь значка «**i**» рядом с названием сети и выберите пункт **Забыть эту сеть** (Forget This Network). В операционной системе Android откройте экран Настройки (Settings), выберите раздел Wi-Fi и, удерживая палец на названии сети, выберите пункт Забыть сеть (Forget Network).

Если вам действительно необходимо сделать что-то конфиденциальное, находясь вне дома, я советую вам в первую очередь подключаться к сотовым сетям передачи данных, вместо того чтобы пользоваться беспроводным соединением в аэропорту или кофейне. Можно также раздавать Интернет со своего мобильного устройства с помощью USB-кабеля, Bluetooth или Wi-Fi. Если вы выбрали Wi-Fi, то обязательно настройте WPA2-шифрование, как уже говорилось ранее. Для путешествий можно купить переносную точку доступа к Интернету. Обратите внимание, что и в этом случае вы не станете невидимыми, но это все равно лучше, чем публичный Wi-Fi-доступ. Но если вы хотите обезопасить себя от слежки со стороны оператора сотовой связи — например, чтобы скачать конфиденциальный документ, — я советую вам пользоваться расширением HTTPS Everywhere или протоколом Secure File Transfer Protocol (SFTP). Протокол SFTP поддерживается приложениями Transmit (iOS) и Tunnelier (Windows).

Технология Virtual Private Network (VPN, виртуальная частная сеть) представляет собой своеобразный защищенный туннель между частной сетью (домашней, рабочей или сетью VPN-провайдера) и вашим устройством, подключенным к общественной сети. Вы можете поискать VPN-сервисы с помощью поисковой системы Google. Средняя годовая стоимость услуг по доступу через VPN составляет порядка 60 долларов США. Интернет-соединению в местной кофейне (или аэропорту, или другом общественном месте) доверять нельзя — это публичная сеть. Но благодаря VPN можно через публичную сеть добраться до защищенной, безопасной. Все, что вы делаете в сети VPN, защищено шифрованием, поскольку весь интернет-трафик передается по защищенным каналам связи, создаваемым поверх общественной сети. Вот почему так важно выбрать надежный VPN-сервис — ведь он видит ваш интернет-трафик. Теперь сомнительный персонаж из кафе увидит только то, что вы подключились к VPN-серверу, и все ваши действия, посещенные сайты и прочие данные будут полностью скрыты от посторонних глаз надежным шифрованием.

Технология Virtual Private Network (VPN, виртуальная частная сеть) представляет собой своеобразный защищенный туннель между частной сетью (домашней, рабочей или сетью VPN-провайдера) и вашим устройством, подключенным к общественной сети.

Однако вы все равно оставите в Интернете след в виде своего IP-адреса, в данном случае это — в вашей домашней или рабочей сети. Так что вы опять-таки не будете невидимыми, даже задействовав VPN. Не забывайте, VPN-провайдер *знает* ваш IP-адрес. Далее я объясню, как сделать это соединение невидимым.

Многие компании предоставляют своим сотрудникам VPN-сервис, чтобы те могли подключаться к частной внутренней корпоративной сети через публичные сети (Интернет). Ну а что же насчет всех остальных?

Существует множество коммерческих VPN-сервисов. Но как узнать, можно ли им доверять? В протоколе IPSec, применяющемся для организации VPN-соединений, априори включена опция PFS (Perfect forward secrecy, Совершенная прямая секретность), но не все сервисы — даже корпоративные — утруждают себя ее настройкой. OpenVPN, полнофункциональная реализация VPN с открытым кодом, включает в себя PFS, поэтому, если сервис заявляет, что использует OpenVPN, можно предположить, что в нем также реализована опция PFS, но не всегда эти ожидания оправдываются. Может оказаться, что OpenVPN не настроено должным образом. Выбирайте сервис, который утверждает, что PFS включена.

Один из недостатков VPN-сервисов заключается в том, что они существенно дороже, чем прокси-серверы. И поскольку коммерческие VPN предназначены для совместного использования, они могут снижать скорость соединения с Интернетом, а в некоторых случаях для вас может просто не оказаться свободного соединения и придется ждать, пока не появится возможность подключиться. Еще одно неудобство связано с тем, что в некоторых случаях Google выдает просьбу ввести код с изображения (CAPTCHA), прежде чем допустить вас до работы с поисковой системой, поскольку сайту необходимо убедиться, что вы человек, а не робот. И наконец, VPN-сервис может хранить статистические данные, поэтому внимательно читайте политику безопасности, чтобы выяснить, не станет ли этот сервис составлять архив с информацией о вашем трафике или историей соединений — пусть даже в зашифрованном виде — и не будут ли подобные сведения доступны правоохранительным органам. Это можно узнать из политики безопасности и пользовательского соглашения. Если сервис может передавать сведения правоохранительным органам, значит, он ведет учет подключений через VPN.

Авиапассажиры, которые пользуются такими веб-сервисами, как GoGo, подвергаются тому же самому риску, что и при подключении к Интернету из кофейни или зала ожидания в аэропорту, и VPN не всегда спасает. GoGo и другие подобные сервисы для подключения к Интернету в самолете запрещают использование приложения Skype и других приложений для голосового общения, поэтому подобные сети не пропускают пакеты UDP — в результате чего большинство VPN-сервисов (которые по умолчанию применяют протокол UDP) работают очень медленно. Однако эту ситуацию можно исправить, выбрав VPN-сервис, в основе которого лежит протокол TCP вместо UDP, например, сервис TorGuard или ExpressVPN. Оба этих VPN-сервиса позволяют пользователю выбирать предпочтительный протокол — TCP или UDP.

Политика безопасности VPN-сервиса также дает серьезную пищу для размышлений. Независимо от того, к какой виртуальной частной сети вы подключаетесь (коммерческой или корпоративной), через эту сеть теперь будет проходить весь ваш трафик, вот почему так важно применять протокол HTTPS. Так VPN-сервис не сможет увидеть содержимое проходящих через него пакетов данных..

Если вы работаете в офисе, возможно, у вашей компании есть своя виртуальная частная сеть, чтобы можно было работать удаленно. В приложении на компьютере вам нужно указать свой логин и пароль (что-то, что вы знаете), а само приложение содержит сертификат идентификации, добавленный туда IT-отделом (что-то, что у вас есть), или оно отправит вам текстовое сообщение на корпоративный телефон (тоже что-то, что у вас есть). А может быть, для подключения потребуются все три пункта (многофакторная аутентификация).

Теперь можно сидеть в кофейне Starbucks или в аэропорту и заниматься рабочими делами, как если бы вы находились дома или в офисе. Однако не стоит решать личные вопросы, например, разбираться со своими банковскими делами, если данный сеанс не зашифрован с помощью расширения HTTPS Everywhere.

Единственный способ перестать сомневаться в надежности VPN-сервиса — сохранять анонимность с самого начала. Если вы действительно стремитесь к полной анонимности, никогда не имейте дел с интернет-соединением, которое можно как-то связать с вами (например, дома, на работе, у друзей, в снятом на ваше имя номере отеля и пр.). В 1990-х меня поймали агенты ФБР, которые отследили сигнал сотового телефона до моей квартиры в Роли, Северная Каролина. Так что никогда не занимайтесь ничем личным с одноразового устройства и не выходите в Интернет с помощью точки доступа, которая как-то к вам относится, если боитесь, что вас могут выслеживать правоохранительные органы. Все, что вы делаете на одноразовом устройстве, не должно никак пересекаться с вашей реальной жизнью. Если хотите быть невидимыми, вы не должны оставлять никаких зацепок, которые могут вывести на вас.

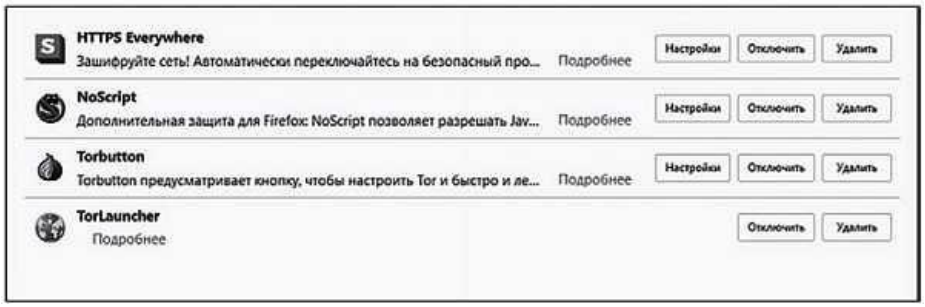
VPN-приложение также можно установить на мобильное устройство. В Интернете можно найти подробные инструкции для устройств Apple и для операционной системы Android.

Если вы следуете всем предложенным мной до сих пор советам, то ваши дела обстоят гораздо лучше, чем у среднего обывателя. Большая часть вашей интернет-активности, вероятно, защищена от отслеживания и манипулирования.

Это касается и используемых вами социальных сетей. Facebook применяет протокол HTTPS в каждой сессии.

Электронная почта? Почта Google также стала поддерживать протокол HTTPS. Большинство сервисов веб-почты последовали этому примеру, как и большинство основных мессенджеров. Да и вообще, большинство крупных сайтов — Amazon, eBay, Dropbox — поддерживают HTTPS.

Чтобы быть невидимым, всегда лучше всего применять многослойную защиту. Риск того, что при подключении к общественной точке доступа ваш трафик попадет в поле зрения посторонних людей, уменьшается с каждым новым слоем защиты. Например, из общественной сети Wi-Fi подключитесь к платному VPN-сервису, а затем подключитесь к сети Tor с помощью браузера Firefox с установленным расширением HTTPS Everywhere.



Тогда все, что вы делаете в Интернете, будет зашифровано и защищено.

Представим себе, что вы хотите просто почитать книгу и не собираетесь заниматься никакими финансовыми операциями или личными делами. И вы выходите в Интернет со своего личного ноутбука вне дома. Кажется, что это безопасно, так? Опять же не вполне. Вам все равно придется принять ряд мер предосторожности.

Во-первых, отключите Wi-Fi. Серьезно. Многие люди не выключают Wi-Fi на компьютере, даже когда Интернет им не нужен. Согласно документам, обнародованным Эдвардом Сноуденом, канадский Центр безопасности коммуникаций (CSEC) может идентифицировать путешественников, перемещающихся через канадские аэропорты, просто перехватывая их MAC-адреса. Эти адреса видны каждому компьютеру, ищущему пробные запросы на подключение, отправляемые беспроводными устройствами. Даже если вы не подключитесь к сети, MAC-адрес устройства будет зафиксирован. Поэтому если вам не нужен Интернет, отключайте Wi-Fi. Как мы видели, ради безопасности и конфиденциальности часто приходится жертвовать удобством.

Уже очень долго мы ходим вокруг да около важного вопроса — вашего MAC-адреса. Он уникален для каждого устройства. И он не фиксирован, его можно изменить.

Давайте я приведу пример.

Во второй главе я рассказывал о том, как скрыть свою электронную переписку с помощью PGP-шифрования. Ну а если вы не хотите разбираться со всеми этими сложностями или у получателя нет публичного ключа PGP? Тогда можно прибегнуть к другому способу ведения тайной электронной переписки: с помощью папки с черновиками в общем электронном ящике.

Именно таким образом бывший директор ЦРУ генерал Дэвид Петреус обменивался письмами со своей любовницей, Полой Бродуэлл, которая также была его биографом. Скандал разразился после того, как Петреус порвал эту связь и заметил, что кто-то шлет одному из его друзей электронные письма с угрозами. Когда ФБР занялось расследованием, агенты обнаружили не только то, что угрозы исходили от Бродуэлл, но и что она также отправляла романтические послания Петреусу.

Уже очень долго мы ходим вокруг да около важного вопроса — вашего MAC-адреса. Он уникален для каждого устройства. И он не фиксирован, его можно изменить.

Интересно то, что Бродуэлл и Петреус не пересылали письма по сети, а оставляли их в папке с черновиками в «анонимном» электронном ящике. В такой ситуации электронное письмо не проходит через чужие серверы, стремясь достичь адресата. Здесь меньше возможностей для перехвата. А если кому-то удастся влезть в ваш ящик, он не найдет там ничего интересного, если вы удаляете черновики и очищаете корзину.

Бродуэлл также заходила в свои «анонимные» электронные ящики с предназначенного специально для этого компьютера. Она не проверяла почту со своего домашнего IP-адреса. Это было бы слишком очевидно. Вместо этого она вела переписку из разных отелей.

Хотя Бродуэлл приложила много усилий, чтобы сохранить секретность, она все равно не стала невидимой. Как написали в газете New York Times, «поскольку аккаунт отправителя был зарегистрирован анонимно, следователям пришлось прибегнуть к компьютерно-технической

экспертизе — включая проверку всех остальных аккаунтов электронной почты, в которые заходили с того же IP-адреса, — чтобы определить, кто был автором этих писем».

Сервисы электронной почты, такие как Google, Yahoo! и Microsoft, хранят данные о входе в аккаунт более года, и эти данные включают в себя информацию об IP-адресе, с которого осуществлялся вход. Например, если вы проверяли почту через общественную Wi-Fi-сеть в кофейне Starbucks, по IP-адресу можно определить географическое местонахождение этого места. Американское законодательство в настоящее время позволяет правоохранительным органам запрашивать подобные сведения у сервиса электронной почты обычной повесткой — участие судьи не требуется.

Следовательно, агенты ФБР выяснили физическое местонахождение каждого IP-адреса, с которого заходили в этот почтовый аккаунт, и сумели вычислить MAC-адрес устройства Бродуэлл, сопоставив данные из журналов маршрутизаторов, установленных в этих местах.

Поскольку расследованием занималось ФБР (это дело имело большое значение, так как Петреус на тот момент был действующим директором ЦРУ), агенты сумели просмотреть журналы маршрутизаторов во всех отелях и узнали, в какое время в каждом из отелей фиксировался MAC-адрес Бродуэлл. Более того, им также удалось обнаружить, что в интересующие их даты Бродуэлл снимала номера в соответствующих отелях. Следователи обратили внимание, что Бродуэлл входила в свою почту, но ни разу не отправила электронное письмо с этих ящиков.

Когда вы подключаетесь к беспроводной сети, MAC-адрес вашего компьютера автоматически фиксируется сетевым оборудованием. Ваш MAC-адрес связан с серийным номером сетевой карты. Чтобы быть невидимым, прежде чем подключаться к какой-либо беспроводной сети, необходимо изменить свой MAC-адрес.

Чтобы оставаться невидимым, нужно менять MAC-адрес перед каждым подключением к беспроводной сети, чтобы ваши интернет-сессии было трудно связать с вами. Также важно в это время не заходить ни в какие личные аккаунты, поскольку иначе вы лишите себя анонимности.

Чтобы изменить MAC-адрес, нужно следовать инструкциям для вашей конкретной операционной системы — Windows, macOS, Linux, Android или iOS. Не забывайте менять MAC-адрес при каждом подключении к общественной (или частной) сети. После перезагрузки возвращается исходный MAC-адрес.

Представим себе, что у вас нет собственного ноутбука и вы вынуждены воспользоваться общественным терминалом. Это может быть в кафе, в библиотеке, даже в бизнес-центре хорошего отеля. Как можно себя защитить?

Когда я отправляюсь в поход с палаткой, я следую принципу «не оставлять следов своего присутствия» — иначе говоря, место, где я разбивал палатку, после моего ухода должно выглядеть точно так же, как когда я пришел. Тот же самый принцип применим и к общественным интернет-терминалам. Когда вы уйдете, никто не должен догадываться, что вы вообще тут были.

Особенно это касается отраслевых выставок. Как-то я побывал на Международной выставке потребительской электроники (Consumer Electronics Show, CES) и увидел там группу публичных интернет-терминалов, предназначенных для того, чтобы посетители выставки, прогуливаясь по залу, могли проверить электронную почту. Я встречал подобное даже на посвященной информационной безопасности ежегодной Коференции RSA в Сан-Франциско. Устанавливать в общественном месте группу публичных терминалов — это плохая идея по ряду причин.

Во-первых, это арендованные компьютеры, которые переходят от мероприятия к мероприятию. Возможно, их почистили, переустановили операционную систему, но возможно, и нет.

Во-вторых, обычно на них запущена система с правами администратора, а это значит, что кто угодно может установить на них любую программу. Например, это может быть вредоносная программа, какой-нибудь клавиатурный шпион, который будет сохранять логины и пароли пользователей. В информационной безопасности существует принцип «минимальных полномочий», согласно которому человек должен получать лишь тот минимум полномочий, которого ему будет достаточно для выполнения своей задачи. Когда вы работаете на общественном терминале с правами системного администратора (а это установка по умолчанию на большинстве подобных терминалов), это нарушает принцип «минимальных полномочий» и повышает риск того, что кто-то до вас успел заразить его вредоносным ПО. Единственный выход — это каким-нибудь образом убедиться, что вы пользуетесь гостевым доступом с ограниченными правами, но большинство людей не знают, как это сделать.

В целом, я советую никогда не доверять общественным интернет-терминалам. Исходите из предположения, что предыдущий пользователь установил на терминал вредоносную программу — умышленно или случайно. Если вы войдете в свою почту Gmail с общественного терминала, на котором стоит клавиатурный шпион, кто-то посторонний получит ваш логин и пароль. Если вы

зайдете в интернет-банк — попрощайтесь со своими деньгами. Не забывайте, что необходимо настраивать двухфакторную аутентификацию на каждом сайте, который посещаете, чтобы хакер, у которого есть ваш логин и пароль, не смог войти в вашу учетную запись. Двухфакторная аутентификация во много раз снижает вероятность взлома аккаунта, даже если хакер узнает ваш логин и пароль.

Что всегда меня удивляет, так это количество людей, пользующихся общественными терминалами на компьютерных конференциях, таких как CES и RSA. Я просто теряю дар речи. В конце концов, если вы на выставке, решайте личные вопросы через канал передачи данных, предоставляемый вашим мобильным оператором, на смартфоне или планшете, обзаведитесь личной точки доступа или просто отложите дела до тех пор, пока не вернетесь домой.

Если вы вынуждены выйти в Интернет вне дома или офиса, возьмите смартфон. Если вам совершенно необходимо воспользоваться публичным терминалом, ни в коем случае не авторизуйтесь в своих личных учетных записях, даже в веб-почте. Если вам, например, необходимо найти какой-то ресторан, заходите только на те сайты, которые не требуют авторизации, например, сервис Yelp или подобные. Если вам приходится прибегать к услугам публичных терминалов регулярно, создайте почтовый ящик специально для них и при необходимости пересылайте с него или на него письма из основных своих ящиков, пока вы в дороге, а оказавшись дома, перестаньте это делать. Так вы сократите объем информации, которая хранится в этом почтовом аккаунте.

Затем убедитесь, что в URL сайтов, которые вы посещаете с помощью общедоступного терминала, присутствует значение https. Если вы его не видите (или видите, но подозреваете, что кто-то изменил адрес, чтобы у вас возникло ложное чувство безопасности), то, вероятно, вам стоит еще раз подумать, прежде чем работать с конфиденциальной информацией через подобный терминал.

Допустим, вы увидели протокол HTTPS в URL. Если это страница авторизации, найдите флажок типа «запомнить меня». Сбросьте его. Понятно почему: это не ваш личный компьютер. На нем будут работать другие люди.

Если система вас запомнит (т. е. вы не сбросите этот флажок), вы создадите на этом устройстве куки. Вы же не хотите, чтобы следующий пользователь терминала увидел вашу почту или получил возможность отправлять письма с вашего ящика, правда?

Как уже упоминалось, не заходите с таких терминалов на сайты финансовых организаций и медицинских учреждений. Если вы авторизовались на некотором сайте (Gmail или другом), обязательно выйдите из аккаунта, когда будете покидать терминал. И рассмотрите возможность позднее в целях безопасности сменить пароль, используя для этого собственный компьютер или мобильное устройство. Может быть, вы не всегда выходите из своих учетных записей дома, но на чужом компьютере это надо делать обязательно.

Когда вы отправили письмо (или сделали что-то другое, не важно), выйдите из аккаунта и очистите историю посещений в браузере, чтобы следующий человек не знал, какие сайты вы посещали. Также сотрите все куки (если есть такая возможность). И убедитесь, что не загрузили на общественный компьютер какой-нибудь свой личный документ. Если загрузили, удалите этот файл (файлы) с рабочего стола или из папки **Загрузки** (Downloads).

К сожалению, просто удалить файл недостаточно. После этого нужно очистить корзину. Это, конечно, не уничтожит файл окончательно — я смогу восстановить его после вашего ухода, если захочу. Но к счастью, большинство людей не я и в большинстве случаев достаточно удалить документ и очистить корзину.

Чтобы быть невидимым, при работе с публичным терминалом необходимо соблюдать все эти меры.

Глава 9

НЕТ ПРИВАТНОСТИ? СМИРИСЬ!

В какой-то момент, скрываясь от властей Белиза, бывший разработчик антивирусного программного обеспечения, Джон Макафи начал вести блог. Как по мне, если вы пытаетесь избежать решетки и хотите полностью раствориться, не нужно начинать вести блог. Хотя бы потому, что вы точно где-то ошибетесь.

Макафи — умный человек. Он заработал свое состояние, став одним из первых разработчиков антивирусного программного обеспечения в те дни, когда Силиконовая долина только начинала развиваться. Затем он продал свою компанию и все свое имущество в США и на протяжении четырех лет, с 2008-го по 2012-й, жил в Белизе, в частном особняке на побережье. И вдруг правительство Белиза взяло его под практически постоянное наблюдение, стало проводить обыски в его доме и выдвинуло обвинение в создании частной армии и контрабанде наркотиков.

Макафи все отрицал. Он заявил, что, наоборот, борется с наркодельцами на острове. Например, он сказал, что предложил мелкому торговцу марихуаной телевизор с плоским экраном в обмен на обещание завязать с наркотиками. Также на слуху случаи, когда он прижимал к обочине машины, в которых, по его подозрениям, находились наркодилеры.

У Макафи действительно была лаборатория, но не факт, что он производил там наркотики. Он утверждает, что занимался разработкой лекарств нового поколения. Поэтому он подозревал, что машины с белыми парнями, проезжавшие мимо его дома, принадлежат шпионам фармацевтических компаний, таких как GlaxoSmithKline. Далее он заявил, что полицейские облавы были спровоцированы фармацевтическими компаниями.

Его собственность охраняли несколько вооруженных человек и одиннадцать собак. Сосед, проживавший двумя домами южнее, Грег Фолл регулярно жаловался местным властям на то, что собаки лают по ночам. Затем одной ноябрьской ночью 2012 года одну из собак Макафи отравили. А чуть позже на той же неделе Фола застрелили. Когда его нашли, он лежал лицом вниз, в луже крови в своем доме.

Власти Белиза, естественно, заинтересовались Макафи, который попал под подозрение. Как Макафи написал в своем блоге, когда он услышал от горничной, что с ним хочет побеседовать полиция, он ударился в бега. Он стал скрываться от правосудия.

Но не блог привел полицию к Макафи. А фотография. И даже не его фотография.

Специалист по безопасности Марк Лавлес (Marc Loveless, он же Simple Nomad) заметил Макафи на фотографии в Twitter, опубликованной журналом Vice в начале декабря 2012 года. На этой фотографии редактор журнала Vice стоял рядом с Макафи в какой-то тропической местности — может быть, в Белизе, а может, где-то еще.

Лавлес знал, что цифровые фотографии содержат много информации о времени, месте и условиях съемки, и хотел посмотреть, что за информацию содержит этот снимок. Цифровые фотографии хранят так называемые EXIF-данные (англ. Exchangeable Image File Format). Это метаданные фотоснимка, там приводятся рутинные подробности, такие как сведения о насыщенности цвета, благодаря которым фотография без искажений отображается на экране или выводится на печать. Также, если позволяет камера, EXIF-данные могут включать в себя точную широту и долготу места съемки.

Стало ясно, что эту фотографию Макафи рядом с редактором журнала Vice сняли с помощью смартфона iPhone 4S. В некоторые смартфоны встроена функция автоматического определения географического местоположения. Лавлесу повезло: выложенный в Интернет файл изображения содержал точное местонахождение Джона Макафи, который, как оказалось, был в соседней Гватемале.

В своем блоге Макафи заявил, что подделал эти данные, но это маловероятно. Позже он сказал, что хотел, чтобы все узнали его местонахождение. Но скорее всего, он просто поленился.

Короче говоря, полиция Гватемалы задержала Макафи и не выпускала из страны. Затем у него начались проблемы со здоровьем, его госпитализировали, и, в конце концов, ему разрешили вернуться в США.

Убийство Грега Фолла так и осталось нераскрытым. Макафи теперь живет в Теннеси, а в 2015 году решил баллотироваться в президенты, чтобы продвигать в правительстве США вопросы киберполитики. Сейчас он редко пишет в блог.

Представим себе, что вы молодой амбициозный джихадист и гордитесь тем, что находитесь на

одной из военных баз ИГИЛ. Что вы сделаете прежде всего? Вы достанете свой смартфон и снимете селфи. Или еще хуже, вы не только сфотографируете себя и свое новое место обитания, но и напишете пару слов о сложных командноштабных машинах в данном пункте дислокации.

На другом краю света военные из авиационного крыла специальных операций в Херлберт-Филд, Флорида, проводят анализ социальных сетей и видят вашу фотографию. «Попался!» — говорит один из них. Через пару часов на новенькое военное сооружение сбрасываются три высокоточные авиационные бомбы. И все это из-за селфи.

Мы не всегда задумываемся о том, что *еще* оказалось на только что созданном нами снимке. В кино или театре это называется «мизансцена», в переводе с французского — «то, что на сцене». На фотографии может быть силуэт большого города, включая вид на Башню свободы из вашего окна. Даже фотография вас в сельском антураже — например, на фоне раскинувшейся до горизонта степи — дает мне представление о том, где вы живете. Эти визуальные подсказки могут стать хорошей зацепкой для тех, кто пытается вас отыскать.

В случае молодого джихадиста в кадр попала военная база.

В метаданных фотографии содержались точные координаты (широта и долгота), или геолокационные данные, того места, где была сделана фотография. Генерал Герберт «Ястреб» Карлайл, глава Боевого авиационного командования ВВС США, подсчитал, что от того момента, когда селфи оказалось в социальных сетях, до того момента, когда военная база была полностью уничтожена, прошло не больше 24 часов.

Безусловно, по метаданным файла изображения можно вас найти. Среди данных EXIF цифрового изображения содержится время и дата съемки, марка и модель фотокамеры и, если на устройстве, с которого сделан снимок, включена геолокация, широта и долгота того места, где была снята фотография. Именно с помощью этой информации американские военные нашли в пустыне военную базу ИГИЛ, подобно тому как Марк Лавлес использовал ее для нахождения Джона Макафи. Любой, кто умеет работать со специальной программой с открытым исходным кодом — это стандартный инструмент под названием **Инспектор** (Inspector) в macOS и доступные для скачивания приложения, такие как FOCA (Windows) или Metagoofil (Linux), — сможет получить доступ к метаданным фотографий и документов.

Иногда местонахождение выдает не фотография, а приложение. Летом 2015 года наркобарон Хоакин Гусман по прозвищу «Эль Чапо» (исп. El Chapo — «коротышка») сбежал из мексиканской тюрьмы и тут же испарился. Или нет?

Через два месяца после побега Эль Чапо из мексиканской тюрьмы строгого режима Альтиплано его 29-летний сын, Хесус Альфредо Гусман Салазар, выложил в Twitter фотографию. Хотя лица двоих мужчин, сидевших за одним столом с Салазаром, были скрыты смайликами, по комплекции мужчина слева был очень похож на Эль Чапо. Более того, Салазар подписал фотографию следующим образом: «Здесь круто, и вы уже поняли, с кем я». К этому посту также были прикреплены сведения о местонахождении — Коста-Рика, — на основании чего можно было сделать вывод, что сын Эль Чапо забыл отключить функцию автоматического указания координат в приложении Twitter на своем смартфоне.

Даже если вам не приходится прятать беглого преступника в своей семье, вы должны знать, что цифровая и визуальная информация, стоящая (иногда на самом виду) за вашими фотографиями, может очень многое рассказать тому, кто вами интересуется.

Фотографии в Интернете могут не только выдать, где вы находитесь. При использовании определенного программного обеспечения они могут стать источником утечки ваших персональных данных.

В 2011 году Алессандро Аквисти, ученый из Университета Карнеги-Меллон, задался следующим вопросом: «Возможно ли с помощью уличного снимка человека определить его номер социального страхования?» И он выяснил, что да. Он взял фотографию случайного студента-волонтера, снятую на простую веб-камеру, и вместе со своей исследовательской группой извлек из нее достаточно сведений, чтобы получить доступ к персональным данным этого человека в Интернете.

Только задумайтесь об этом. Можно взять фотографию случайного человека с улицы и с помощью программы для распознавания лиц попытаться идентифицировать его личность. Без подтверждения от самого человека можно ошибиться и даже не узнать об этом. Но велика вероятность, что большинство попаданий будут точными.

«Онлайновый и оффлайновый миры смешиваются друг с другом, а ваше лицо — это проводник, связующее звено между двумя мирами», — рассказал Аквисти изданию Threatpost. «Я думаю, что мы получили суровый урок. Нам придется принять тот факт, что само понятие неприкосновености частной жизни постепенно стирается. Вы лишились своей приватности на улице или в толпе.

Засилье технологий меняет наше биологически заложенное ожидание приватности».

В ходе исследования Аквисти и остальные члены группы останавливали студентов на территории кампуса Университета Карнеги-Меллон и просили их пройти онлайн-опрос. Пока они этим занимались, веб-камера ноутбука фотографировала студента и этот снимок тут же передавался программе распознавания лиц. Когда студент заканчивал проходить опрос, на мониторе появлялось несколько его фотографий из сети. Почти 42 процента фотографий были определены верно и взяты из тех профилей Facebook, которые действительно принадлежали людям, заполнявшим анкету.

Если у вас есть аккаунт Facebook, вы, вероятно, уже знаете, что эта социальная сеть применяет технологию распознавания лиц. Загрузите на сайт фотографию, и Facebook попытается отметить на ней людей из списка ваших друзей, ваших знакомых. Вы можете до определенной степени контролировать этот процесс. Зайдя в настройки аккаунта Facebook, можно установить такой режим, чтобы сервис уведомлял вас о том, что собирается отметить людей на снимке, и чтобы вы сами решали, отмечать ли вас. Также можно настроить сервис так, чтобы он спрашивал вас, хотите ли вы поделиться фотографией, например на стене или в ленте, или нет.

Чтобы фотографии, на которых вы отмечены на Facebook, были никому не видны, откройте настройки аккаунта, перейдите на вкладку **Конфиденциальность** (Privacy Settings). Там множество настроек, например, можно установить, чтобы фотографии были видны только вам. Что касается всего остального, то Facebook пока не предоставляет возможности запретить другим пользователям отмечать вас на фотографиях без вашего разрешения.

Такие компании, как Google и Apple, также встраивают технологию распознавания лиц в некоторые из своих приложений, например Google Фото и Apple Фото. Возможно, имеет смысл изучить настройки конфиденциальности таких приложений и сервисов, чтобы ограничить возможности технологии распознавания лиц в каждом конкретном случае. Компания Google до сих пор воздерживалась от включения технологии распознавания лиц в свой сервис «Google Картинки» (маленький значок фотоаппарата в правой части поисковой строки Google). Можно загрузить какое-нибудь изображение, и Google найдет похожие изображения, но не станет искать другие фотографии с тем же человеком, что и на загруженном снимке. Представители Google многократно подчеркивали, что, предоставив людям возможность идентифицировать незнакомцев по фотографии, мы «перейдем черту».

И все-таки правительства некоторых тоталитарных государств это проделывали. Они фотографировали протестующих на массовых антиправительственных митингах, а затем выкладывали фотографии в Интернет.

Им помогало не столько программное обеспечение для распознавания лиц, сколько краудсорсинг. Также в некоторых штатах Америки подозреваемых в преступных деяниях искали через базу фотографий регистрационно-экзаменационного отдела автоинспекции. Но это сложная процедура с участием ресурсов, которыми располагает штат. Что мог сделать одинокий ученый?

Аквисти и его коллеги хотели посмотреть, сколько данных о человеке с фотографии можно найти в Интернете. Чтобы это выяснить, они применяли технологию распознавания лиц от компании Pittsburgh Pattern Recognition (или PittPatt), которую позже приобрела корпорация Google. Алгоритмы, реализованные в технологии PittPatt, были лицензированы государственными учреждениями и компаниями, работающими в сфере безопасности. Вскоре после покупки технологии компания Google снова озвучила свои намерения: «Как мы уже говорили на протяжении года, мы не станем добавлять распознавание лиц в поиск Google, если не сможем придумать надежную модель защиты конфиденциальности. Пока нам это не удалось». Будем надеяться, что компания сдержит свое слово.

Проводя свое исследование, Аквисти мог пользоваться технологией PittPatt в сочетании с информативными профилями на Facebook, т. е. теми, где волонтеры из числа студентов Университета Карнеги-Меллон разместили свои фотографии наряду с дополнительными сведениями о себе. Затем ученые сравнили фотографии с изображениями в «анонимных» профилях на популярных сайтах знакомств. В таких профилях исследователи сумели идентифицировать 15 процентов якобы «анонимных» виртуальных сердцеедов.

Однако самой дерзкой целью эксперимента было установить номер социального страхования человека, имея только его фотографию. Для этого Аквисти и его группа искали профили на Facebook, в которых была указана дата и город рождения человека. В предыдущем эксперименте в 2009 году те же ученые показали, что одной этой информации было достаточно для получения номера социального страхования (номера социального страхования присваиваются по формуле, которая зависит от конкретного штата, а с 1989 года номера социального страхования стали присваиваться в день рождения или в очень близкую к нему дату, благодаря чему угадать последние четыре цифры номера теперь еще проще).

Произведя первоначальные подсчеты, ученые отправляли каждому студенту дополнительный

опросный лист, целью которого было выяснить, в каких случаях полученные с помощью их алгоритма первые пять цифр номера социального страхования были верными. И они оказывались верными в большинстве случаев.

Могу поспорить, что у вас есть фотографии, которые вы не хотите видеть в Интернете. Вполне возможно, вы не сможете убрать их оттуда, даже если удалите их из своего аккаунта в социальной сети. Отчасти это обусловлено тем, что, выложив что-нибудь в социальную сеть, вы теряете контроль над этим контентом и он оказывается в руках социальной сети. И вы согласились на это, когда приняли условия пользовательского соглашения.

Если вы пользуетесь популярным приложением Google Фото, даже удалив фотографию, не стоит рассчитывать, что с ней покончено. Пользователи обнаружили, что фотографии никуда не исчезают, даже после удаления приложения с мобильного устройства. Почему? Потому что когда изображение попадает в «облако», оно утрачивает зависимость от приложения, в том смысле, что другие приложения тоже получают к нему доступ и могут по-прежнему показывать изображение даже после того, как вы его удалили у себя.

Это оказывает определенное влияние на реальный мир. Допустим, вы добавили дурацкую подпись к фотографии человека, который теперь работает в той компании, куда вы хотите устроиться. Или вы выложили свою фотографию с неким человеком, а теперь не хотите, чтобы ваш теперешний супруг (или супруга) узнал о нем. Пусть это и ваш личный профиль, но контент попадает в распоряжение социальной сети.

Вероятно, вы никогда не утруждали себя чтением пользовательского соглашения ни на одном из сайтов, куда выкладываете свои личные данные, где делитесь каждодневными событиями, мыслями, чувствами, историями, жалобами, недовольством и так далее или где вы совершаете покупки, играете, учитесь, общаетесь, возможно, ежедневно или даже ежечасно. Для регистрации в большинстве социальных сетей необходимо принять их условия пользовательского соглашения. Не известно, насколько это законно, но в этих пользовательских соглашениях часто присутствуют пункты, в соответствии с которыми сайт может хранить данные пользователей и даже делиться ими с третьими лицами.

Уже много лет у людей возникает целый ряд вопросов к Facebook и его политике в отношении хранения данных. Например, их смущает то, что пользователям сложно удалить свой аккаунт. И в этом отношении сеть Facebook не одинока.

Множество веб-сайтов прописывают в своем пользовательском соглашении приблизительно такие же условия, которые, скорее всего, отпугнули бы вас от сайта, если бы вы их прочитали, прежде чем согласиться. Вот пример с сайта Facebook от 19 марта 2018 года:

Вам принадлежит весь контент и информация, которые вы публикуете на Facebook, и вы можете контролировать их передачу с помощью настроек конфиденциальности и приложений. Кроме того:

1. Вы прямо предоставляете нам следующее разрешение с учетом ваших настроек конфиденциальности и приложений в отношении использования всего контента, на который распространяются права на интеллектуальную собственность, такого как фото и видео (далее — «контент ИС»): вы предоставляете нам неисключительную, не требующую лицензионных выплат, действующую по всему миру лицензию с правом передачи и выдачи сублицензий на использование любого контента ИС, который вы публикуете на Facebook или в связи с ним (далее — «Лицензия на ИС»). Настоящая Лицензия на ИС прекращает действие, когда вы удаляете опубликованный вами контент ИС или свой аккаунт, за исключением случаев, когда другие лица делятся вашим контентом и не удаляют его.

Другими словами, социальная сеть имеет право поступать по своему усмотрению со всем, что вы выкладываете на сайт. Она даже может продавать ваши фотографии, ваши мнения, ваши тексты и вообще все, что вы публикуете, зарабатывая деньги на ваших материалах, не отдавая вам ни копейки. Администрация соцсети может использовать любой ваш комментарий, критическое замечание, мнение, жалобу или сплетню (если вы такое практикуете) и даже самые личные сведения о вас, вашей жизни, ваших детях, вашем начальнике или о вашем любовнике. И этот контент не обязательно будет использоваться анонимно: если вы указали свое настоящее имя, социальная сеть может сделать то же самое.

Все вышесказанное означает, что среди прочего изображения, выложенные на Facebook, могут перекочевать на другие сайты. Если у вас есть какие-то особенно позорные фотографии и вы хотите выяснить, не разлетелись ли они по всему миру, можно произвести так называемый обратный поиск изображения в Google. Для этого щелкните по маленькому значку в виде фотоаппарата в поисковой строке Google и загрузите любую фотографию с жесткого диска. Через несколько минут вы увидите все сайты, на которых размещено это изображение. Теоретически, если на фотографии изображены вы, то вам следует знать обо всех сайтах, указанных в списке результатов. Однако если вы

выясните, что кто-то выложил фотографию на сайт, который вам не нравится, вы мало что сможете сделать.

Обратный поиск изображения ограничивается уже опубликованными изображениями. Другими словами, если изображение немного отличается, система Google его не найдет. Она найдет обрезанные версии изображения, но при условии, что центральная или просто довольно большая его часть останется без изменений.

Однажды на мой день рождения кто-то попытался сделать печать с моей фотографией. У компании, куда этот человек обратился, Stamps.com, очень строгие правила в отношении использования фотографий осужденных преступников. Мою фотографию забраковали. Вероятно, сотрудники выполнили в Интернете поиск по изображению.

Моя фотография находилась в одной базе данных, где было указано мое имя (Кевин Митник) и что я осужден по такому-то делу.

Через год моя подруга попробовала прислать этой компании более раннюю мою фотографию с другим именем, которая была сделана еще до того, как я получил известность. Она посчитала, что этой фотографии могло вовсе не быть в Интернете. И угадайте, что произошло? Это сработало. Вторую фотографию с молодым мной одобрили. Это яркий пример несовершенства поиска по изображению.

Иными словами, если вы найдете свои фотографии, которые не хотели бы выкладывать, у вас есть несколько вариантов.

Во-первых, свяжитесь с сайтом. У большинства сайтов есть электронные адреса в духе . Можно также обратиться к администратору с помощью адреса электронной почты . Объясните, что вы владелец изображения и не давали разрешения на его публикацию. Большинство администраторов уберут фотографию без лишних проблем. Однако при необходимости можно выслать официальный DMCA-запрос (англ. Digital Millennium Copyright Act — закон об авторском праве в цифровую эпоху) на адрес электронной почты .

Будьте осторожны. Ложный DMCA-запрос может навлечь на вас неприятности с законом, поэтому, если вы вынуждены прибегнуть к этой мере, сначала проконсультируйтесь с юристом. Если фотографию все равно не удаляют, попробуйте пойти дальше и обратиться к хостинговой компании, обслуживающей сайт (Comcast, GoDaddy или другой компании). Большинство из них с большим вниманием относятся к DMCA-запросам, если они соответствуют закону.

Что еще есть в вашем профиле, кроме фотографий? Вы бы не стали рассказывать все подробности своей жизни человеку, который просто сел рядом с вами в метро. Точно так же не следует раскрывать слишком много сведений о себе на обезличенном сайте. Никогда не знаешь, кто просматривает твой профиль. Выложив информацию, вы уже не сможете вернуть все обратно. Хорошо подумайте, чем именно вы наполняете свой профиль — вовсе не обязательно заполнять все предложенные поля, например, давать информацию об университете (и о том, когда вы его окончили). По сути, нужно заполнять как можно меньше полей.

Аналогичным образом следует поступать в отношении «социальных сетей». Нет необходимости обманывать, можно просто намеренно напускать туман. Например, если вы выросли в Атланте, пишите «Юго-восток США» или просто «Я с юга».

Чтобы еще больше скрыть свою личность, можно указать «безопасную дату рождения», которая на самом деле не является реальной. Обязательно запоминайте свои безопасные даты рождения, поскольку иногда дату рождения нужно назвать сотруднику службы поддержки или указать для входа на сайт после блокировки.

После создания или внесения изменений в свой профиль в социальной сети, потратьте пару минут на то, чтобы проверить настройки конфиденциальности аккаунта. Например, на сайте Facebook нужно настроить проверку публикаций, на которых вы отмечены. В настройке «Кто может видеть публикации, в которых вы отмечены, в вашей хронике?» выберите значение «Только я». Предлагать такие рекомендации друзьям — это плохая идея, верно же? Запретите друзьям отмечать вас в каких-либо посещенных местах.

Родители должны добавляться в друзья к своим детям и следить за их постами, а в идеале заранее обсудить с ними, что можно выкладывать, а что нельзя.

При регистрации аккаунта на Facebook, вероятно, больше всех стараются дети. Они стремятся заполнить каждое пустое поле, даже дать информацию о том, состоят ли они в отношениях с кем-нибудь. Или бездумно указывают номер школы, в которой учатся, имена учителей и номера автобусов, которыми они ездят каждое утро. Хотя эти сведения не включают в себя точный адрес проживания, но могут на него указать. Родители должны добавляться в друзья к своим детям и следить за их постами, а в идеале заранее обсудить с ними, что можно выкладывать, а что нельзя.

Невидимость вовсе не означает, что вы из соображений безопасности не должны публиковать вообще никакой информации о своей жизни. Рассказывать о себе можно, но необходимо руководствоваться здравым смыслом и периодически заглядывать в настройки безопасности своего аккаунта — поскольку политика конфиденциальности нередко меняется, иногда не в лучшую сторону. Не разглашайте свою дату рождения, даже выдуманную, или хотя бы скройте ее от тех «друзей» на Facebook, с которыми вы лично не знакомы.

Представим себе, что кто-то выложил пост о том, что миссис Санчес — отличная учительница. Следующий пост рассказывает о ярмарке ремесел в начальной школе Аламо. Через поиск Google можно найти информацию о том, что миссис Санчес — учительница пятых классов в начальной школе Аламо, из чего можно сделать вывод о том, что владелец аккаунта — десятилетний школьник.

Несмотря на многократные предупреждения Союза потребителей и других подобных организаций, люди продолжают выкладывать всю информацию о себе в Интернет. Не забывайте, что третьи лица имеют законное право пользоваться этими данными, раз вы выложили их в общественный доступ.

Также не забывайте, что никто не заставляет вас рассказывать о себе. Вы можете выкладывать столько личных сведений, сколько считаете нужным. В некоторых случаях требуется указать какие-то конкретные данные. Делиться ли чем-то сверх этого необходимого минимума, решать вам. Вы должны сами понять, какой уровень конфиденциальности для вас приемлем, а также осознать, что любая выложенная в Интернет информация подобна воробью из пословицы — если один раз вылетела, уже не поймаешь.

Чтобы помочь вам определиться, в мае 2015 года сайт Facebook запустил новый инструмент проверки настроек конфиденциальности. Несмотря на наличие подобных средств проверки, почти 13 миллионов пользователей Facebook никогда не применяли их или вообще не слышали об их существовании (по результатам опроса издания Consumer Reports в 2012 году). А 28 % пользователей предоставляли доступ ко всем или почти всем своим постам на стене не только своим друзьям, но и более широкой аудитории (по результатам того же опроса). И все же 25 % опрошенных заявили, что указали ложную информацию в своих профилях, чтобы скрыть свою личность, и эта цифра выросла в два с половиной раза по сравнению с 2010 годом. По крайней мере, мы хоть чему-то научились.

Хотя вы имеете право выкладывать не совсем точную информацию о себе, имейте в виду, что, например, в Калифорнии незаконно писать в Интернете под чужим именем. Нельзя, скажем, притворяться каким-то другим, действительно существующим человеком. А по правилам Facebook, вы не можете создать аккаунт под именем, отличным от настоящего.

Это правило коснулось и меня лично. Мой аккаунт на Facebook был заблокирован, потому что администрация сайта решила, что я выдаю себя за Кевина Митника, им не являясь. В тот момент на Facebook было двенадцать Кевинов Митников. Исправить ситуацию удалось только после того, как на сайте CNET опубликовали историю о том, что на Facebook заблокировали настоящего Кевина Митника.

Однако существует множество причин, по которым человеку может понадобиться выйти в Интернет под чужим именем. Если у вас возникла такая необходимость, найдите социальную сеть, где можно общаться анонимно или под псевдонимом. Однако такие сайты далеко не соответствуют Facebook по величине аудитории и масштабу.

Если в друзья просится незнакомец, подумайте как следует. Конечно, можно удалить человека из друзей в любой момент, но у него все равно появится шанс изучить ваш профиль — злоумышленнику нужна всего пара секунд, чтобы влезть в вашу жизнь. Лучший совет здесь — выкладывать на Facebook как можно меньше персональной информации, поскольку часто люди подвергаются очень изощренным атакам, в том числе и через аккаунты своих друзей в социальных сетях.

А данные, которые видят ваши друзья, могут быть переданы ими кому-то еще без вашего ведома и согласия.

Обращайте особое внимание на то, кого вы добавляете в друзья. Если вы знаете человека в реальной жизни, отлично. Или если это друг человека, которого вы знаете в реальной жизни, то допустимо. Но если в друзья просится незнакомец, подумайте как следует. Конечно, можно удалить человека из друзей в любой момент, но у него все равно появится шанс изучить ваш профиль — злоумышленнику нужна всего пара секунд, чтобы влезть в вашу жизнь.

Лучший совет здесь — выкладывать на Facebook как можно меньше персональной информации, поскольку часто люди подвергаются очень изощренным атакам, в том числе и через аккаунты своих друзей в социальных сетях. А данные, которые видят ваши друзья, могут быть переданы ими кому-то

еще без вашего ведома и согласия.

Приведу пример. Как-то меня хотел нанять мужчина, который стал жертвой вымогательства. С ним произошло следующее: на сайте Facebook он познакомился с красивой девушкой и начал отправлять ей свои обнаженные фотографии. Это продолжалось какое-то время. Затем в один прекрасный день ему сказали, что он должен заплатить этой женщине, которая могла на самом деле быть каким-то парнем из Нигерии, 4000 долларов. Он заплатил, но когда с него потребовали еще 4 тысячи, угрожая иначе послать эти фотографии всем его друзьям на Facebook, включая родителей, он обратился ко мне. Он не знал, что ему делать. Я сказал, что единственное, что в его силах, — это рассказать обо всем своим родным или просто ждать, станут ли вымогатели выполнять свои угрозы. Я посоветовал ему перестать платить, потому что шантажист не оставит его в покое, пока он платит.

Любой аккаунт в социальной сети может быть взломан: кто-то мог добавиться к вам в друзья только для того, чтобы подобраться поближе к одному из ваших знакомых. Сотрудник правоохранительных органов может искать информацию о человеке, который по случайному стечению обстоятельств оказался в списке ваших друзей. Такое случается.

Согласно данным Фонда электронных рубежей (EFF), социальные сети уже много лет служат федеральным агентам инструментом негласного наблюдения за людьми.

В 2011 году организация EFF выложила в сеть 38-страничный документ (полученный в соответствии с законом о свободе информации (США)), который, как утверждалось, был частью учебного курса ФБР по ведению расследований с помощью социальных сетей. Хотя федеральные агенты по закону не могут притворяться теми, кем не являются, они могут добавиться к вам в друзья. Так они смогут просмотреть все ваши посты (в зависимости от настроек конфиденциальности), а также публикации всех ваших друзей. Фонд электронных рубежей продолжает изучать скользкие моменты, связанные с этим новым методом слежки со стороны правоохранительных органов.

Иногда за вами могут начать следить или просто наблюдать крупные корпорации. Например, если вы опубликуете или твитнете что-то, что им покажется оскорбительным — даже вполне невинный отзыв о пройденном вами тесте. Для одного школьника подобный твит оказался источником больших неприятностей.

Когда с Элизабет С. Джуитт, директором старшей школы Уотчунг Хиллз в Уоррене, штат Нью-Джерси, связалась компания, которая разрабатывала экзаменационные тесты для этой школы, ее реакцией было скорее удивление, чем беспокойство. Она была удивлена тем, что эта компания (Pearson Education) следит за профилем в социальной сети Twitter, принадлежащим одному из учеников ее школы. Ученикам младших классов предоставляется определенная степень свободы и право на конфиденциальность в том, что касается их публикаций в социальных сетях. Но начиная со средней школы и дальше (вплоть до университета), дети должны понимать, что все, что они делают в социальных сетях, становится достоянием общественности и может привлечь ненужное внимание. В данном случае один из учеников Элизабет Джуитт, как утверждалось, выложил в Twitter вопросы из стандартного теста.

На самом деле мальчик выложил вопрос о вопросе — не фотографию страницы теста, а просто пару слов — из обычного контрольного среза для школьников штата Нью-Джерси. Твит появился в Интернете около 15:00 — намного позже того времени, когда школьники округа сдавали экзамен. После беседы директора с родителями ученика тот удалил свой пост. Ситуация была никак не связана со списыванием. Опубликованный вопрос — он не разглашается — был скорее субъективным комментарием, нежели обращением за подсказкой.

Но поведение компании Pearson возмутило людей. «Министерство образования проинформировало нас, что Pearson следит за всеми социальными сетями во время проведения тестирования PARCC (Partnership for Assessment of Readiness for College and Careers, оценка готовности к обучению в колледже и получению профессии)», — написала Джуитт в электронном письме своим коллегам, которое местные СМИ опубликовали без ее разрешения. В нем Джуитт подтвердила, что компания Pearson доложила в Министерство образования еще как минимум о трех подобных инцидентах.

И Pearson не единственная компания, которая отслеживает посты в социальных сетях на предмет попыток кражи своей интеллектуальной собственности. Такое поведение вызывает вопросы. Например, каким образом компания установила личность школьника, опубликовавшего пост в Twitter? Издание New York Times опубликовало следующее заявление Pearson: «К утечке данных относятся и все те случаи, когда кто-нибудь делится информацией о тесте за пределами классной комнаты — от обычных разговоров до постов в социальных сетях. Опять же наша цель — гарантировать честное тестирование для всех учащихся. У всех школьников должна быть возможность сдавать тест на равных условиях с остальными».

Журналисты New York Times выяснили через официальных лиц в Массачусетсе, где также

проводится тестирование PARCC, что компания Pearson сверяет твиты о своих тестах со списком школьников, сдающих стандартизированный тест. По этому пункту компания Pearson отказалась давать комментарии.

Власти штата Калифорния также много лет следили за социальными сетями детей, сдающих ежегодный тест STAR (Standardized Testing and Reporting, стандартизированное тестирование и отчет). В 2013 году, когда в штате последний раз проводилось это тестирование, Министерство образования Калифорнии выявило 242 школы, ученики которых выложили в социальные сети публикации, касающиеся тестирования, во время проведения самого теста, из которых только 16 содержали непосредственные вопросы из теста или ответы на них.

«Инцидент выявил то, до какой степени школьники находятся под наблюдением как в школе, так и за ее пределами», — сказала Элана Зейде, научный сотрудник, занимающийся вопросами информационной безопасности в Институте информационного законодательства на базе Нью-Йоркского университета. «Социальные сети обычно воспринимаются как нечто, не связанное со школой. Twitter больше коррелируется с общением вне школы, поэтому данные, которые собирала компания Pearson, — это скорее беседы по пути из школы домой, чем разговоры в школьных коридорах».

Однако далее она говорит: «Фокус беседы тоже должен смещаться от персональных интересов и обид к более глобальным последствиям выкладывания информации в аккаунте. Школы и организации должны перестать обвинять родителей в чрезмерной подозрительности на том лишь основании, что они не могут четко объяснить, какой именно вред был нанесен их ребенку. Родители в свою очередь должны понимать, что школы не могут ставить интересы конфиденциальности на первое место, поскольку также существуют и общественные интересы, пожертвовав которыми можно навредить системе образования как таковой».

Сервис Twitter со своим ограничением длины сообщения в 140 символов также сумел широко раскинуть свои щупальца, собирая множество крошечных подробностей о нашей повседневной жизни. Политика безопасности этого сервиса уведомляет пользователей, что он собирает — и сохраняет — личную информацию через различные сайты, приложения, SMS-сообщения, сервисы, API (application programming interface, интерфейс прикладного программирования) и другие сторонние источники. Когда человек пользуется сервисом Twitter, он дает сервису согласие на сбор, хранение, обработку, раскрытие и другое применение персональной информации. Чтобы зарегистрироваться там, необходимо указать свое имя, логин, пароль и адрес электронной почты. На один электронный ящик можно зарегистрировать только один аккаунт Twitter.

Сервис Twitter со своим ограничением длины сообщения в 140 символов также сумел широко раскинуть свои щупальца, собирая множество крошечных подробностей о нашей повседневной жизни.

Другой сомнительный с точки зрения конфиденциальности момент, связанный с Twitter, касается утечки закрытых твитов. Это происходит, когда друзья человека с закрытым аккаунтом ретвитят, или копируют, частные публикации этого человека в открытый аккаунт. Слово — не воробей.

Персональной информацией в любом случае опасно делиться в Twitter, особенно если ваши твиты «открыты» (по умолчанию). Не указывайте там свой адрес, номер телефона, данные банковской карты или номер социального страхования. Если вам необходимо поделиться персональной информацией, пишите нужному человеку напрямую через личные сообщения. Но помните, что даже защищенные твиты или личные сообщения могут быть опубликованы в открытом доступе.

Для современной молодежи, так называемого поколения Z, Facebook и Twitter — уже устаревшие сервисы. Поколение Z на своих мобильных устройствах в основном отдает предпочтение приложениям WhatsApp (который, по иронии судьбы, теперь является частью Facebook), Snapchat (не Facebook), Instagram и Instagram Истории (тоже принадлежит Facebook). Все эти приложения в основном сосредоточены вокруг визуальной составляющей — в том смысле, что в них можно или просто выкладывать свои фотографии и видео, или смотреть чужие фотографии и видео.

Приложение для обмена фотографиями и видео Instagram — это альтернатива Facebook для более молодой аудитории. Оно позволяет подписываться на обновления других пользователей, ставить лайки, оставлять комментарии и общаться через личные сообщения. Политика приложения Instagram предусматривает внимательное отношение к поступающим от пользователей и правообладателей просьбам удалить нежелательный контент.

Snapchat не принадлежит компании Facebook и, вероятно, поэтому выделяется на фоне остальных приложений. Snapchat позиционируется как приложение, позволяющее пересылать другим пользователям самостоятельно уничтожающиеся фотографии. Время хранения фотографии ограничено, в среднем оно составляет две секунды, и этого достаточно ровно для того, чтобы получатель успел взглянуть на изображение. К сожалению, двух секунд вполне хватает на то, чтобы сделать снимок экрана, который сохраняется в памяти устройства.

Зимой 2013 года две малолетние школьницы из Нью-Джерси сфотографировались обнаженными и отправили эти фотографии мальчику из своей школы через приложение Snapchat. Разумеется, они предполагали, что изображение автоматически удалится через две секунды после отправки. По крайней мере, так обещали разработчики.

Однако мальчик умел делать скриншоты сообщений Snapchat. Полученные снимки он выложил в свой Instagram-аккаунт. Instagram не удаляет фотографии через две секунды. Стоит ли говорить, что фотографии с обнаженными подростками стали вирусными и директору школы пришлось разослать родителям всех детей записки с просьбой удалить снимки девочек со смартфонов школьников, иначе у них возникнут проблемы с законом в связи с хранением детской порнографии. Что касается тех трех учеников, с которых все началось, то им не могли выдвинуть обвинения по причине малолетства, но каждый из них получил дисциплинарное взыскание на уровне школьного округа.

Не только девочки могут отправлять свои обнаженные фотографии мальчикам. В британской школе четырнадцатилетний мальчик через Snapchat отправил свои интимные снимки девочке из той же школы, опять же считая, что изображение исчезнет через пару секунд. Девочка же сделала снимок экрана, и… ну вы понимаете, чем все закончилось. Согласно сообщению BBC, эти мальчик и девочка будут внесены в британскую базу сексуальных преступников несмотря на то, что они слишком малы и не подлежат уголовной ответственности.

Как и WhatsApp с его несовершенной системой размывания удаленных фотографий, приложение Snapchat, несмотря на все заверения разработчиков, на самом деле не удаляет изображения. В действительности в 2014 году разработчикам Snapchat пришлось согласиться с обвинениями Федеральной торговой комиссии и признать, что компания обманывала пользователей, обещая им, что сообщение просто исчезнет. Правительственное агентство выяснило, что эти сообщения можно сохранять или восстанавливать по прошествии времени. Политика безопасности компании Snapchat также гласит, что приложение никогда не запрашивает, не отслеживает и не обрабатывает геолокационные данные вашего устройства, однако Федеральная торговая комиссия выяснила, что и эти заявления ложны.

Для регистрации в любом веб-сервисе пользователь должен быть старше 13 лет (включительно). Именно поэтому подобные сервисы спрашивают дату вашего рождения. Однако пользователь может на свой страх и риск заявить, что ему больше 13 лет или 21 года и т. д. Родители, которые узнали, что их десятилетние дети зарегистрированы в Snapchat или Facebook, могут заявить о нарушении и добиться удаления учетной записи. С другой стороны, родители, которые хотят, чтобы у их детей был аккаунт в социальной сети, часто меняют год рождения ребенка. Эти данные становятся частью цифровой личности ребенка. Внезапно ваш десятилетний ребенок превращается в четырнадцатилетнего, а значит, ему будут показывать рекламные объявления, предназначенные для более взрослых детей. И обратите внимание на то, что каждый их адрес электронной почты и каждая опубликованная на сервисе фотография будут зафиксированы.

Приложение Snapchat также передает геолокационные данные устройства под управлением операционной системы Android, основанные на информации от Wi-Fi-провайдера и оператора сотовой связи, своему сервису вебаналитики. Если у вас устройство под iOS и вы указали свой номер телефона, чтобы найти друзей, Snapchat добавит в свою базу имена и номера телефонов из вашей адресной книги, не ставя вас в известность, хотя перед первым импортом контактов iOS все-таки запросит у вас разрешение. Мой вам совет — выбирайте другое приложение, если вам нужна настоящая конфиденциальность.

В Северной Каролине одному старшекласснику и его девушке предъявили обвинения в хранении фотографий обнаженных детей несмотря на то, что это были их собственные фотографии, которыми они обменялись по взаимному согласию. Девушке предъявили два обвинения в растлении малолетних: одно — за то, что она сделала фотографию, а второе — за то, что хранила ее. Отбросив в сторону обмен эротическими фотографиями, мы получаем то, что в Северной Каролине закон запрещает подросткам снимать самих себя в обнаженном виде и хранить эти фотографии. В полицейском протоколе девушка представлена и как жертва, и как преступница.

Парню предъявили пять обвинений, по два на каждую из его собственных фотографий и одно — за хранение фотографии своей девушки. Если бы его осудили по этим пунктам, он мог бы получить 10 лет тюрьмы и состоял бы в базе сексуальных преступников до конца своих дней. И все за то, что сфотографировал себя в обнаженном виде и сохранил подобную фотографию, присланную ему его девушкой.

Когда я учился в старших классах школы, я мог просто пригласить на свидание девушку, с которой только что познакомился. В наше время приходится выкладывать информацию о себе в Интернет, чтобы люди могли понять, с кем имеют дело. Но будьте осторожны.

А если вы заходите в свою учетную запись на сайте знакомств с чужого компьютера или вам вдруг пришлось воспользоваться для этого публичным интернет-терминалом, всегда выходите из

аккаунта. Это важно. Вы же не хотите, чтобы кто-нибудь нажал на кнопку возврата на предыдущую страницу в браузере и увидел информацию о ваших романтических знакомствах. Или внес изменения в ваш профиль. Также не забывайте сбрасывать флажок «запомнить меня» на странице авторизации. Иначе посторонний человек сможет автоматически войти в ваш аккаунт с этого компьютера.

Приложения для знакомств могут выдавать ваши геолокационные данные, отчасти это предусмотрено их функциями. Допустим, вы хотите встретиться с кем-то, кто вам нравится, и вы обращаетесь за помощью к приложению, которое подскажет, далеко ли этот человек от вас в данный момент. Мобильное приложение для знакомств Grindr предоставляет очень точную информацию о местонахождении своих пользователей… возможно, даже слишком точную.

Предположим, вы собираетесь на первое свидание, а может быть, на второе. Люди не всегда показывают свое истинное лицо на первых двух свиданиях. Как только человек станет вашим другом на сайте Facebook или подпишется на вас в Twitter или в любой другой социальной сети, он сможет увидеть всех ваших друзей, все фотографии, все интересы. ситуация может выйти из-под контроля очень быстро.

Мы поговорили об веб-сервисах, как насчет мобильных приложений?

Приложения для знакомств могут выдавать ваши геолокационные данные, отчасти это предусмотрено их функциями. Допустим, вы хотите встретиться с кем-то, кто вам нравится, и вы обращаетесь за помощью к приложению, которое подскажет, далеко ли этот человек от вас в данный момент. Мобильное приложение для знакомств Grindr предоставляет очень точную информацию о местонахождении своих пользователей. возможно, даже слишком точную.

Колби Мур и Патрик Уордл, сотрудники фирмы Synack, занимающейся кибербезопасностью, сумели подделать запросы к приложению Grindr и проследить за перемещениями нескольких подписчиков по городу. Они также обнаружили, что, если искать одного и того же человека с трех разных аккаунтов, можно произвести триангуляцию полученных результатов и получить более точное представление о местонахождении человека в данный момент.

Пускай вы не пользуетесь приложениями для знакомств, но просто зарегистрировавшись в сервисе Yelp с целью найти хороший ресторан, вы передаете сторонней организации информацию о вашей половой принадлежности, возрасте и местонахождении. По умолчанию приложение может отправлять сведения в ресторан в следующем виде — «женщина, 31 год, из Нью-Йорка, просматривала отзывы». Можно открыть настройки и изменить их на «базовые» (Basics), тогда заведение будет получать только информацию о вашем городе (к сожалению, полностью отключить эту опцию не получится). Возможно, лучший способ этого избежать — не авторизоваться, а пользоваться сервисом Yelp просто как гость.

Прежде чем соглашаться на загрузку любого приложения для Android, сначала ознакомьтесь со списком его разрешений.

Вообще, что касается геолокации, очень рекомендую вам проверить, отправляют ли *какие-либо* из установленных на вашем устройстве приложений данные о вашем текущем местонахождении. В большинстве случаев можно отключить эту функцию, либо в каждом приложении по-отдельности, либо на устройстве в целом.

Прежде чем соглашаться на загрузку любого приложения для Android, сначала ознакомьтесь со списком его разрешений. Эти разрешения можно посмотреть в магазине Google Play, для этого необходимо открыть информацию о приложении, прокрутить страницу вниз и найти раздел под названием **Разрешения** (Permissions).

Если что-то из этих разрешений вас смущает или вам кажется, что разработчик приложения получает слишком много полномочий, просто не устанавливайте его. Компания Apple не предоставляет подобной информации о своих приложениях в AppStore, а вместо этого при необходимости приложения запрашивают разрешение на то или иное действие. Лично я предпочитаю устройства под управлением операционной системы iOS, поскольку операционная система всегда спрашивает разрешение, прежде чем выдавать мою личную информацию — например, сведения о моем местонахождении. Кроме того, операционная система iOS гораздо лучше защищена, чем Android (конечно, если вы используете iPhone или iPad без джейлбрейка). Разумеется, злоумышленники с большим бюджетом могут купить эксплойты для любой операционной системы на рынке, но эксплойты для iOS стоят дороже всех остальных — свыше миллиона долларов.

Лично я предпочитаю устройства под управлением операционной системы iOS, поскольку операционная система всегда спрашивает разрешение, прежде чем выдавать мою личную информацию — например, сведения о моем местонахождении.

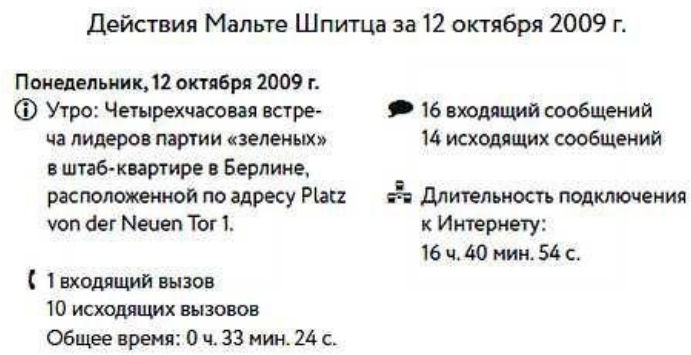
Глава 10

МОЖЕШЬ БЕЖАТЬ, НО ТЕБЕ НЕ СКРЫТЬСЯ

Если вы целый день ходите с сотовым телефоном, как большинство людей, то вы не невидимы. Вы под наблюдением — даже если у вас на смартфоне отключена функция геолокации. Например, если вы пользуетесь устройством под управлением операционной системы iOS8.2 или более ранней версии, в авиарежиме функция геолокации отключается автоматически, но если у вас более новая версия iOS, как у большинства из нас, функцию геолокации надо выключать самостоятельно — даже в авиарежиме, если, конечно, вы не приняли других мер. Чтобы выяснить, насколько хорошо оператор сотовой связи осведомлен о его ежедневных перемещениях, известный немецкий политик Мальте Шпитц возбудил иск против мобильного оператора, и немецкий суд потребовал от компании выдать зафиксированные данные. Сам объем этих данных поражал воображение. Всего за полгода оператор зафиксировал местонахождение Шпитца 85 000 раз, при этом записывая каждый входящий и исходящий вызов абонента, номера телефонов его собеседников и длительность каждого разговора. Другими словами, там содержались метаданные, полученные со смартфона Шпитца. И речь идет не только о голосовых вызовах, но и о текстовых сообщениях.

Если вы целый день ходите с сотовым телефоном, как большинство людей, то вы не невидимы. Вы под наблюдением — даже если у вас на смартфоне отключена функция геолокации.

Шпитц обратился к другим организациям за помощью в форматировании и публикации данных. Одна из организаций скомпоновала данные по дням, как на рисунке ниже. Место проведения утренней встречи членов партии «зеленых» было установлено на основании данных о широте и долготе, полученных из отчетов оператора.



Другая организация составила анимированную карту всех перемещений господина Шпитца по Германии за этот день с точностью до минуты, а также отметила мигающими значками все точки, где он совершал или принимал телефонные вызовы. Такого удивительного уровня детализации удалось достичь всего за несколько рабочих дней.

Конечно, сбор данных по господину Шпитцу — это отнюдь не уникальная ситуация, и такое происходит не только в Германии. Это всего лишь яркий пример того, какие данные о вас хранит оператор сотовой связи. И эта информация может использоваться в судебных процессах.

В 2015 году в Апелляционный суд четвертого округа США поступило дело, для разбирательства которого потребовались аналогичные данные от оператора сотовой связи. Дело касалось двух преступников, ограбивших банк, магазин 7-Eleven, несколько ресторанов быстрого питания и ювелирный магазин в Балтиморе. Получив от оператора Sprint координаты смартфонов главных подозреваемых за период в 221 день, полицейские сумели связать этих людей с серией совершенных преступлений, опираясь на территориальную близость мест преступления друг к другу, а также на близость самих подозреваемых к этим местам преступления.

Подробности другого подобного дела, которое разбиралось в Федеральном окружном суде Северного округа Калифорнии, не раскрываются, однако известно, что оно также было построено на «исторической информации оператора сотовой связи», предоставленной компаниями Verizon и AT&T. Цитируя Американский союз защиты гражданских свобод (англ. American Civil Liberties Union, ACLU), который выносил свое консультативное заключение по этому делу, такие данные «становятся источником практически постоянного учета местонахождения и перемещения человека». Согласно протоколам судебного заседания, когда федеральный судья во время слушания в Калифорнии упомянул о конфиденциальности телефонного общения, федеральный обвинитель «ответил, что владельцы мобильных телефонов, беспокоящиеся о вопросах конфиденциальности, могут либо не брать с собой телефон, либо отключать его».

Создается впечатление, что при этом нарушается предусмотренное Четвертой поправкой (к

Конституции США) право на защиту от необоснованных обысков. Большинство людей никогда бы не разглядели взаимосвязь между ношением мобильного телефона и нарушением своего права не подвергаться слежке со стороны правительства. Но в наши дни дела обстоят именно так. Как в первом случае (операторы Verizon и AT&T), так и во втором (Sprint) политика конфиденциальности сотовой компании не объясняла пользователям, насколько подробными данными об их местоположении она будет обладать. Более того, оператор AT&T в своем письме к Конгрессу США в 2011 году сообщил, что хранит собранные данные на протяжении пяти лет «на случай судебных разбирательств».

Данные о перемещениях хранятся не только оператором, но и производителем устройства и разработчиком ПО. Например, ваш аккаунт Google сохраняет все геолокационные данные с устройства на операционной системе Android. Точно так же Apple ID хранит все данные об устройстве iPhone. Чтобы защитить свою конфиденциальность, периодически нужно удалять геолокационные данные со смартфона. Если у вас операционная система Android, коснитесь значка **Настройки** (Settings) и выберите пункт **Google**. Выберите пункт **Местоположение —> История местоположений —> Управление действиями** (Location —> Google Location History —> Manage Activities). В открывшемся приложении Google Карты коснитесь кнопки  и выберите пункт **Настройки** (Settings), а затем коснитесь кнопки **Удалить всю историю местоположений** (Delete all Location History).

Что касается аккаунта Google, то, если не отключить геолокацию, все сведения будут доступны в Интернете и с их помощью можно восстановить ваши перемещения поминутно. Например, большую часть дня вы можете провести в одной точке, а затем вдруг начать активно ездить по городу, встречаясь с клиентами или выбравшись за едой. Самое неприятное заключается в том, что, если кто-нибудь когда-нибудь доберется до вашего аккаунта Google или Apple ID, он, посмотрев, где вы находитесь основную часть времени, сможет определить, где вы живете, кто ваши друзья и даже каков ваш распорядок дня.

Для устройства под управлением операционной системы iOS необходимо сделать следующее: коснитесь значка **Настройки** (Settings) и выберите пункт **Конфиденциальность —> Службы геолокации** (Privacy —> Location Services), прокрутите вниз и коснитесь пункта **Системные службы —> Часто посещаемые места** (System Services —> Frequent Locations), затем коснитесь пункта **Очистить историю** (Clear Recent History).

Что касается аккаунта Google, то, если не отключить геолокацию, все сведения будут доступны в Интернете и с их помощью можно восстановить ваши перемещения поминутно. Например, большую часть дня вы можете провести в одной точке, а затем вдруг начать активно ездить по городу, встречаясь с клиентами или выбравшись за едой. Самое неприятное заключается в том, что, если кто-нибудь когда-нибудь доберется до вашего аккаунта Google или Apple ID, он, посмотрев, где вы находитесь основную часть времени, сможет определить, где вы живете, кто ваши друзья и даже каков ваш распорядок дня.

Таким образом, мы выяснили, что в наше время простая прогулка превращается в море возможностей проследить, чем вы занимаетесь. Допустим, что, зная это, вы постоянно оставляете сотовый телефон дома. Так вы решите проблему слежки, верно? Не обязательно.

Вы носите фитнес-трекеры, такие как браслет Jawbone UP (компании Fitbit) или FuelBand (Nike)? Если нет, может быть, у вас смарт-часы Apple, Sony или Samsung? Если вы пользуетесь чем-нибудь из перечисленного — фитнес-браслетом и/или смарт-часами, — то ваши перемещения легко можно отследить. Эти устройства и сопровождающие их приложения разработаны для того, чтобы регистрировать ваши действия часто с помощью сигналов спутниковой системы навигации. Данные могут передаваться в режиме реального времени или могут быть загружены позже, но в любом случае ваши перемещения регистрируются.

Апологет конфиденциальности Стив Мэнн ввел новый термин «*обратное наблюдение*» (англ. sousveillance, образовано от англ. surveillance (наблюдение) и фр. sous (под)). Этот термин означает, что за нами следят не сверху, например, другие люди, камеры слежения и пр., а «снизу» — небольшие устройства, которые мы берем с собой, а может быть, даже надеваем на себя.

Фитнес-трекеры и смарт-часы фиксируют биометрические параметры, такие как пульс, количество сделанных шагов, даже температуру тела. В магазине App Store можно найти множество независимых приложений для наблюдения за самочувствием и состоянием здоровья с помощью смартфонов и часов компании Apple. То же самое относится и к магазину Google Play Store. И (вот сюрприз!) эти приложения пересылают компании данные под предлогом того, что владельцу устройства они могут позже понадобиться, но также для того, чтобы передавать их дальше — иногда без вашего явно выраженного согласия.

Например, во время велогонки «Эмджен-Тур» в Калифорнии (англ. Amgen Tour of California) в 2015 году участники могли посмотреть, кто их обогнал, а позже в Интернете отправить им личное сообщение. Довольно странно, когда посторонний человек пишет тебе о конкретном маневре,

который ты выполнил во время гонки и который ты мог и не запомнить.

Похожий случай произошел со мной. На шоссе из Лос-Анджелеса в Лас-Вегас меня подрезал незнакомый мне водитель на BMW. Копаясь в своем телефоне, он внезапно перестроился и проскочил в нескольких сантиметрах от меня, напугав меня до одури. Он чуть не убил нас обоих.

Я схватил сотовый телефон и позвонил в отдел регистрации транспортных средств, представившись сотрудником правоохранительных органов, чтобы по номеру машины выяснить его имя, адрес и номер социального страхования. Далее я позвонил в сотовую компанию AirTouch, представившись ее сотрудником, и по его номеру социального страхования мне нашли номер его сотового телефона.

Всего минут через пять после того, как этот водитель меня подрезал, я позвонил ему. Меня до сих пор трясло, я был взбешен и зол. Я закричал: «Слышь, ты, дебил, я тот чувак, которого ты подрезал пять минут назад, когда чуть не убил нас обоих. Я из автоинспекции, и если ты выкинешь еще один такой номер, останешься без водительских прав!»

Наверное, он до сих пор не может понять, как другой водитель на шоссе сумел узнать его номер телефона. Надеюсь, мой звонок заставил его стать повнимательнее на дороге. Хотя как знать.

Но эта история вернулась ко мне бумерангом. Со мной произошло вот что: однажды мой аккаунт AT&T (оператор сотовой связи) взломали какие-то скрипт-кидди (так называют не слишком грамотных хакеров), применив методы социальной инженерии. Хакер позвонил в магазин AT&T на Среднем Западе и представился сотрудником другого магазина AT&T. Он убедил служащего сменить адрес электронной почты, привязанный к моему аккаунту, чтобы сбросить пароль и получить доступ к информации из моей учетной записи, включая данные обо всех платежах!

Что касается велогонки в Калифорнии, ее участники обменивались друг с другом персональными данными с помощью включенной по умолчанию функции Flyby приложения Strava. В интервью изданию Forbes Гэрет Неттлтон, глава международного маркетинга в компании Strava, сказал: «Strava — это принципиально открытая платформа, которая объединяет спортсменов и общество в целом. Однако конфиденциальность наших участников очень важна для нас, и мы предприняли меры, направленные на то, чтобы спортсмены могли с легкостью регулировать настройки приватности».

И у Strava действительно есть расширенные настройки приватности, позволяющие регулировать, кому показывать частоту сердцебиения. Также можно обозначить конфиденциальные области, чтобы другие не видели, где вы живете или работаете. Если бы во время велогонки спортсмены отключили функцию Flyby, их информация была бы отмечена как «конфиденциальная».

У остальных средств фитнес-трекинга присутствуют похожие настройки безопасности. Возможно, у вас сложилось впечатление, что раз вы не увлекаетесь велоспортом и не собираетесь подрезать других во время пробежки на пешеходной дорожке рядом со своим офисом, то вам нечего опасаться. Однако вы делаете что-то другое, может быть, довольно личное, о чем также могут узнать посторонние через приложение и веб-сайт, поэтому вопросы конфиденциальности касаются и вас.

Сам по себе учет таких действий, как сон или подъем по ступенькам, особенно когда он ведется с определенной целью, например, для снижения суммы страховых взносов, вероятно, не может скомпрометировать вашу конфиденциальность. Но объединив эти данные с другими сведениями, можно получить о вас более целостную картину. И не исключено, что столько информации о себе вы раскрывать не хотите.

Компания Fitbit, производитель устройства, включала секс в журнал учета ежедневных физических нагрузок. Эти данные, хоть и в анонимном виде, индексировались поисковой системой Google до тех пор, пока ситуация не получила огласку.

Один владелец фитнес-трекера, просматривая свои данные в Интернете, обнаружил, что каждый раз во время занятий сексом у него фиксировалось сильное учащение сердцебиения. Как выяснилось, компания Fitbit, производитель устройства, включала секс в журнал учета ежедневных физических нагрузок. Эти данные, хоть и в анонимном виде, индексировались поисковой системой Google до тех пор, пока ситуация не получила огласку. Компания быстро исключила эти сведения из журналов.

Кто-то может подумать: «Ну и что?» Действительно, как таковая эта информация не очень интересна. Но если объединить данные о частоте сердцебиения, скажем, с геолокационными данными, ситуация начинает приобретать любопытную окраску. Репортер издания Fusion Кашмир Хилл показал один из худших вариантов возможного применения данных с устройств Fitbit, задав себе вопрос: «Что, если бы страховые компании объединили данные о вашей физической активности с данными геолокации, но не для того, чтобы узнать, когда вы занимаетесь сексом, а чтобы узнать *где*? Может ли страховая компания (речь идет о медицинской страховке) выявить

клиента, который делал это в нескольких разных местах в течение одной недели, и повысить коэффициент риска для этого человека лишь на основании его неразборчивости в связях?»

С другой стороны, данные Fitbit успешно применяются в судебных слушаниях в качестве доказательств вины или ее отсутствия в тех ситуациях, которые раньше считались тупиковыми. Яркий пример: данные Fitbit помогли доказать, что женщина солгала об изнасиловании.

Во время посещения Ланкастера, штат Пенсильвания, женщина сообщила полиции, что проснулась посреди ночи и обнаружила в своей постели незнакомца. Далее она заявила, что потеряла свое устройство Fitbit, пытаясь освободиться. Когда полиция нашла Fitbit и дама разрешила полицейским просмотреть данные, сложилась совсем иная картина. Судя по всему, женщина бодрствовала всю ночь. Как рассказали по местному телевидению, ей предъявили обвинения в ложном доносе в полицию, ложном вызове службы спасения и фальсификации доказательств, поскольку она, как утверждает полиция, намеренно перевернула мебель и подкинула нож на место преступления, чтобы создавалось впечатление, будто бы в дом вломился насильник.

Помимо прочего, фитнес-трекеры — это также хорошее подспорье в делах об утрате трудоспособности. Канадская юридическая фирма, опираясь на данные фитнес-трекера, доказала тяжелые последствия травмы, полученной ее клиентом на рабочем месте. Клиент передал данные устройства Fitbit, которые демонстрировали явное снижение активности, в аналитическую фирму Vivametrica, которая берет данные с носимых устройств и сравнивает их с уровнем активности и показателями здоровья населения в целом. «До сих пор нам всегда приходилось полагаться только на клинические исследования, — рассказал журналу Forbes Саймон Мюллер из юридической фирмы McLeod в Калгари. — Теперь мы анализируем более длительные промежутки времени в течение дня и располагаем достоверными данными».

Даже если у вас нет фитнес-трекера, ваша конфиденциальность может пострадать из-за смарт-часов, таких как Galaxy Gear компании Samsung. Если на дисплее часов всплывают уведомления о новых сообщениях, письмах и телефонных вызовах, другой человек также сможет их увидеть и прочитать.

Даже если у вас нет фитнес-трекера, ваша конфиденциальность может пострадать из-за смарт-часов, таких как Galaxy Gear компании Samsung. Если на дисплее часов всплывают уведомления о новых сообщениях, письмах и телефонных вызовах, другой человек также сможет их увидеть и прочитать.

Недавно большую популярность обрело устройство GoPro, крошечная камера, которая крепится к шлему или приборной панели вашего автомобиля для записи данных о ваших перемещениях. Но что случится, если вы забудете пароль от своего мобильного приложения GoPro? Исследователь из Израиля одолжил камеру GoPro у своего друга, и ему нужно было войти в привязанный к ней аккаунт в мобильном приложении, но он не знал пароль. Как и в электронной почте, в приложении GoPro можно сбросить пароль. Однако тогда этот процесс был явно недоработанным — впоследствии недостатки устранили. Приложение GoPro отправляло на электронную почту пользователя ссылку для восстановления пароля, но фактически это была ссылка для скачивания ZIP-файла, который необходимо было загрузить на SD-карту устройства. Когда исследователь открыл ZIP-файл, он увидел там текстовый файл под названием «настройки», в котором содержались данные пользователя — включая идентификатор SSID и пароль от GoPro, с помощью которого устройство подключалось к Интернету. Исследователь обнаружил, что, если изменить номер в ссылке — 8605145 — на какой-нибудь другой, например 8604144, можно получить доступ к настройкам чужих устройств GoPro, включая чужие пароли.

Можно утверждать, что обсуждение проблем конфиденциальности началось — или по крайней мере стало интересным — благодаря компании Eastman Kodak, созданной в конце XIX века. Вплоть до того времени фотография была серьезным, отнимающим много времени, физически тяжелым занятием, для которого нужно было специальное оборудование (камеры, осветительные приборы, лаборатории), а люди должны были подолгу неподвижно сидеть в студии. Затем появилась компания Kodak, которая предложила компактную и относительно недорогую камеру — Kodak. Первый фотоаппарат стоил 25 долларов — в наше время это около 100 долларов. В дальнейшем компания Kodak разработала фотоаппарат Brownie, который продавался по цене 1 доллар. Обе камеры можно было брать с собой и делать снимки вне дома и офиса. По сути, это портативные компьютеры и смартфоны своего времени.

Внезапно люди оказались в такой ситуации, что у любого человека на пляже или в общественном парке может быть с собой камера и кто угодно может случайно попасть в кадр. Появилась необходимость хорошо выглядеть. Приходилось вести себя соответственно. «Нужно было изменить свое отношение не просто к фотографии, а к тому, что вы фотографируете, — говорит Брайан Уоллис, бывший главный куратор Международного центра фотографии. — Вам приходилось тщательно обставлять ужин, готовить декорации для вечеринки в честь дня рождения».

Я считаю, что мы и правда ведем себя иначе, когда за нами наблюдают. Большинство из нас

старается вести себя наилучшим образом, когда мы знаем, что на нас направлен объектив камеры, хотя, разумеется, всегда найдутся те, кому это абсолютно безразлично.

Возникновение фотографии также повлияло на отношение людей к своей приватности. Теперь любое непристойное поведение могло быть запечатлено на фото. Сейчас нас окружают видеорегистраторы и нагрудные камеры, которые активно применяются правоохранительными органами, чтобы всегда было документальное свидетельство наших поступков в случае нарушения закона. В наши дни существует технология распознавания лиц, поэтому можно сфотографировать человека, а затем по этой фотографии найти его профиль в социальной сети Facebook. В наши дни мы делаем селфи.

Но в 1888 году вездесущая фотокамера стала шокирующим и неприятным новшеством. Издание Hartford Courant затрубило тревогу: «Добропорядочный гражданин не может оказаться замешанным в каком-нибудь конфузе без риска быть запечатленным в этот момент на фотографии, которая потом попадет в руки его учеников в воскресной школе. И молодой человек, который хочет уединиться со своей любимой девушкой, плавая на лодке по реке, должен постоянно прикрываться зонтиком».

Некоторые люди восприняли перемены в штыки. В 1880-х группа американок, путешествуя поездом, разбила чужой фотоаппарат, поскольку они не хотели, чтобы их фотографировали. В Великобритании подростки объединялись в группы и ходили по пляжам, запугивая любого, кто пытался сфотографировать женщин, выходящих из воды после купания в океане.

В 1890-х Сэмюэль Уоррен и Луис Брандейс — последний в дальнейшем стал членом Верховного суда — написали статью, в которой говорилось, что «Моментальная фотография и газетная индустрия посягнули на неприкосновенные границы частной и домашней жизни». Они предложили на законодательном уровне ввести понятие частной жизни и, отчасти чтобы уменьшить волну сделанных тайком фотографий, установить ответственность за любое вторжение в нее. Подобные законы были приняты в нескольких штатах.

К нашему времени уже несколько поколений выросло в условиях постоянного риска попасть в объектив фотокамеры и оказаться на моментальном снимке — вам говорит о чем-нибудь название Polaroid? Но теперь нам также приходится иметь дело с *повсеместным распространением* фотографии. Куда бы вы ни пошли, вас могут снять на фото или видео, не спрашивая согласия. И эти фотографии может увидеть кто угодно в любой точке мира.

Наше отношение к неприкосновенности частной жизни заключает в себе противоречие. С одной стороны, мы очень ее ценим, считаем ее чем-то само собой разумеющимся и воспринимаем ее как неотъемлемую составляющую нашей свободы и независимости: разве не должно все, чем мы занимаемся за закрытыми дверями своего дома, оставаться нашим личным делом? С другой стороны, люди любопытны. И теперь мы получили такие богатые возможности для утоления своего любопытства, как никогда раньше.

Вам когда-нибудь было интересно, что там за забором через дорогу, в соседском дворе? Практически во всех подобных случаях узнать ответ на этот вопрос можно с помощью новых технологий. Благодаря производителям беспилотников, таким как 3D Robots или CyPhy, любой человек может купить себе дрон (например, у меня квадрокоптер DJI Phantom 4).

Наше отношение к неприкосновенности частной жизни заключает в себе противоречие. С одной стороны, мы очень ее ценим, считаем ее чем-то само собой разумеющимся и воспринимаем ее как неотъемлемую составляющую нашей свободы и независимости: разве не должно все, чем мы занимаемся за закрытыми дверями своего дома, оставаться нашим личным делом? С другой стороны, люди любопытны. И теперь мы получили такие богатые возможности для утоления своего любопытства, как никогда раньше.

Вам когда-нибудь было интересно, что там за забором через дорогу, в соседском дворе? Практически во всех подобных случаях узнать ответ на этот вопрос можно с помощью новых технологий. Благодаря производителям беспилотников, таким как 3D Robots или CyPhy, любой человек может купить себе дрон (например, у меня квадрокоптер DJI Phantom 4). Дроны — это беспилотные летательные аппараты с дистанционным управлением. Они устроены гораздо сложнее, чем те устройства, которые раньше можно было купить в магазинах электроники. Почти все они оснащены крошечными видеокамерами. Они позволяют посмотреть на мир по-новому. Некоторыми дронами можно управлять с мобильника.

Персональный дрон — это любопытная Варвара в квадрате. Теперь, когда вы можете парить на высоте нескольких десятков метров над землей, для вас почти нет недостижимых границ.

В настоящий момент страховые компании применяют дроны в коммерческих целях. Только задумайтесь об этом. Если вы оценщик страховых убытков и хотите получить представление о состоянии собственности, которую собираетесь застраховать, можно просто запустить туда дрон,

который поможет осмотреть территорию и получить видеозапись. Можно поднять его высоко в небо и наслаждаться обзором, прежде доступным только с вертолета.

Персональный дрон — это современное средство подглядывания за соседями. Мы можем просто запустить его над крышей чужого дома и посмотреть, что внизу. Вдруг у соседей есть бассейн? Вдруг им нравится купаться нагишом? Все стало сложнее: мы рассчитываем на неприкосновенность частной жизни, находясь у себя дома, на своей территории, однако теперь обеспечить ее не так просто. Например, компания Google замазывает лица, номера машин и другую персональную информацию при сборе данных для таких сервисов, как Google Планета Земля и Google Просмотр улиц. Но сосед с личным дроном не даст вам таких гарантий — хотя вы можете попробовать вежливо попросить его не запускать дрон над вашим домом. Дрон с видеокамерой заменит вам сервисы Google Планета Земля и Google Просмотр улиц вместе взятые.

Конечно, существуют некоторые правила. Например, Федеральное управление гражданской авиации США выпустило свод предписаний, согласно которому дрон не должен покидать зону видимости оператора, не должен подлетать к аэропорту ближе, чем на определенное расстояние, и не должен летать выше определенного уровня над землей. Определить допустимую зону полета для вашего дрона можно с помощью специального приложения B4UFLY. Кроме того, в ответ на применение дронов в коммерческих целях несколько штатов выпустили законы, запрещающие или серьезно ограничивающие их использование. Рядовым жителям Техаса запрещено применять дроны, хотя есть несколько исключений: например риэлторы. Самую либеральную позицию в отношении дронов заняло правительство штата Колорадо, которое официально разрешило жителям отстреливать пролетающие в небе аппараты.

Правительство США как минимум должно принудить владельцев дронов регистрировать свои игрушки.

В Лос-Анджелесе, где я живу, чей-то дрон повредил линию электропередач в районе Западного Голливуда на пересечении улицы Ларраби и бульвара Сансет. Если бы дрон был зарегистрирован, власти бы сумели найти того, кто заставил 700 человек несколько часов обходиться без света, в то время как десятки сотрудников энергетической компании были вынуждены работать всю ночь, чтобы восстановить подачу электроэнергии.

Розничные магазины все чаще пытаются лучше узнать своих покупателей. Один из достаточно эффективных способов это сделать заключается в применении IMSI-перехватчиков для сотовых телефонов. Когда вы заходите в магазин, IMSI-перехватчик получает информацию о вашем сотовом телефоне и определяет его номер. После этого система сможет отправить запросы в десятки баз данных и составить ваш профиль.

Оффлайновые магазины также используют технологию распознавания лиц в своих точках продаж. Это своего рода замена швейцару на входе.

«Здравствуйте, Кевин», — в недалеком будущем, возможно, именно такое стандартное приветствие я буду слышать от сотрудников магазина, в котором раньше ни разу не бывал. Персонализация процесса посещения магазина — это очередная, хоть и очень прозрачная, форма слежки. Мы больше не можем совершать покупки анонимно.

В июне 2015 года, всего через две недели после того, как Конгресс США принял «Акт о свободе США» (видоизмененную версию «Патриотического акта» с небольшими доработками в отношении неприкосновенности частной жизни), девять организаций по защите прав потребителей, некоторые из которых горячо поддерживали «Акт о свободе США», шокированные поведением нескольких крупных магазинов, отказались продолжать переговоры, целью которых было ограничение применения технологии распознавания лиц.

Камнем преткновения стал вопрос о том, должны ли компании в обязательном порядке спрашивать у покупателей разрешение на сбор информации о них. Звучит разумно, однако ни один из крупных розничных продавцов, участвующих в переговорах, не был готов пойти на этот шаг. По их словам, если человек заходит в магазин, он автоматически становится объектом для изучения и сбора данных.

Кому-то, возможно, понравится такой «персонализованный» подход к посещению магазина, но большинство из нас будет чувствовать себя неуютно. Магазины видят ситуацию иначе. Они не хотят давать покупателям выбор, поскольку хотят вычислить воришек, которые попросту откажутся от прохождения идентификации, дай им такую возможность. Если же распознавание лиц будет производиться автоматически, то уже попадавшиеся воры будут распознаваться прямо на входе в магазин.

Что говорят покупатели? По крайней мере, в Великобритании семь из десяти опрошенных считают использование технологии распознавания лиц в магазине «чем-то нездоровым». А в США некоторые штаты, такие как Иллинойс, взяли сбор и хранение биометрических данных под свой контроль. Эти

законы стали благодатной почвой для судебных исков. Например, житель Чикаго подал в суд на Facebook из-за того, что веб-сервис применял технологию распознавания лиц для идентификации этого человека на чужих фотографиях без его разрешения.

С помощью технологии распознавания лиц идентифицировать человека можно просто по его фотографии. А если вы и так знаете, кто этот человек, и просто хотите проверить, находился ли он там, где должен был находиться? Это еще один вариант применения данной технологии.

Моше Гриншпан — генеральный директор израильско-американской компании Face-Six, которая занимается системами распознавания лиц. Их программное обеспечение Churchix используется — помимо прочего — для учета прихожан в церквях. Суть в том, чтобы помочь церквям выяснить, кто из прихожан посещает церковь нерегулярно, и мотивировать их приходить чаще, а также определить постоянно посещающих службы прихожан и стимулировать их жертвовать церкви больше денег.

Как утверждает компания Face-Six, она обслуживает не менее 30 церквей по всему миру. Церкви нужно лишь загрузить высококачественные фотографии прихожан. Затем система начинает вести учет посещений этими людьми служб и мероприятий.

Когда журналист из издания Fusion спросил у Гриншпана, сообщают ли церкви своим прихожанам, что за ними следят, тот ответил: «Не думаю, что церкви об этом говорят людям. Мы стараемся их к этому подтолкнуть, но сомневаюсь, что они это делают».

Джонатан Зиттрейн, директор Центра Интернета и общества Беркмана и Кляйна при юридическом факультете Гарвардского университета, пошутил, что для людей нужно придумать специальный тег «nofollow», вроде того, который применяется на некоторых сайтах. Это защитит людей, которые не хотят, чтобы их фотографии появились в базах системы распознавания лиц. С этой целью японский Национальный институт информатики разработал «козырек приватности». Очки, стоимость которых будет в районе 240 долларов, генерируют свет, который может увидеть только камера. В области глаз создается своего рода световой экран, чтобы обмануть систему распознавания лиц. По результатам первых испытаний, очки помогают обойти систему распознавания лиц в 90 процентах случаев. Единственное неудобство заключается в том, что их нельзя носить во время управления автомобилем или езды на мотоцикле. Возможно, они не будут выглядеть модно. Но это отличный способ реализовать свое право на неприкосновенность частной жизни в общественном месте.

Зная, что в общественных местах о неприкосновенности частной жизни говорить не приходится, возможно, вы будете спокойнее себя чувствовать, оставаясь в своей машине, дома или в офисе. К сожалению, это больше не выход. В следующих нескольких главах я расскажу почему.

Глава 11

ЭЙ, КИТТ*, НЕ РАССКАЗЫВАЙ, ГДЕ Я

У специалистов по безопасности Чарли Миллера и Криса Валасека уже был опыт взлома автомобильных систем. Ранее эти двое проникли в бортовой компьютер автомобиля Toyota Prius — но при этом они сначала физически подключились к автомобилю и сидели на его заднем сиденье. Позже, летом 2015 года, Миллер и Валасек сумели захватить управление автомобилем Jeep Cherokee, который ехал по шоссе в Сент-Луисе на скорости свыше 110 км/ч. Они управляли машиной удаленно, находясь на большом расстоянии от нее.

За рулем данного джипа сидел репортер издания Wired Энди Гринберг. Исследователи заранее предупредили Гринберга: что бы ни происходило, не паникуй. Оказалось, что это непростая задача, даже для человека, который знал, что его машину взломали.

«Внезапно перестала работать педаль газа, — написал Гринберг, делясь своими впечатлениями. — Я лихорадочно нажимал на педаль и смотрел, как падают обороты двигателя, скорость джипа снизилась наполовину, а затем машина вообще стала ползти. Это произошло как раз в тот момент, когда я оказался на эстакаде и нельзя было съехать на обочину. Эксперимент перестал быть забавным».

Впоследствии исследователей подвергли критике за «безумное» и «опасное» поведение. Джип Гринберга был среди других машин на дороге, а не на испытательном полигоне, поэтому правоохранительные органы штата Миссури на момент написания данной книги собирались предъявить обвинение Миллеру, Валасеку и, возможно, Гринбергу.

Об удаленном взломе «подключенных» машин говорят уже очень давно, но только эксперимент Миллера и Валасека заставил автомобильную промышленность обратить внимание на эту проблему. Этот инцидент можно воспринимать как угодно — как «виртуозную хакерскую атаку» или как полноправный эксперимент, — но в любом случае он заставил производителей автомобилей серьезно задуматься о кибербезопасности, а также о том, должен ли Конгресс США на законодательном уровне запретить хакерский взлом автомобилей.

Другие исследователи показали, что могут перепрограммировать протокол, управляющий чужим автомобилем, перехватив и проанализировав GSM- или CDMA-трафик бортового компьютера этой машины. Им удалось взломать систему управления автомобилем с помощью SMS-сообщений: в частности они смогли открывать и закрывать двери автомобиля. Кому-то даже удалось этим способом проникнуть в систему дистанционного запуска двигателя. Но Миллер и Валасек были первыми, кто сумел дистанционно перехватить полное управление машиной. И, как они утверждают, таким же образом они могут получить контроль над автомобилями и в других штатах.

Возможно, самым важным результатом эксперимента Миллера и Валасека стало то, что компания Chrysler отозвала более 1,4 млн своих автомобилей из-за проблем с программным обеспечением — первый подобный случай в истории. В качестве временной меры она также приостановила подключение отозванных автомобилей к сети Sprint, через которую машины передают и получают данные от производителя в режиме реального времени. Миллер и Валасек рассказали на конференции DEF CON23, что убедились, что это возможно — захватывать машины в других штатах, — но они знали, что это противоречит нормам морали. Поэтому они решили не взламывать чужую машину, а провести эксперимент в контролируемых условиях в родном городе Миллера с Гринбергом за рулем.

В данной главе мы поговорим о том, насколько уязвимы для кибератак машины, которыми мы управляем, поезда, на которых мы ездим, и мобильные приложения, с помощью которых мы добираемся до пункта назначения, а также о многочисленных пробелах в нашей конфиденциальности, связанных с «подключенными» автомобилями.

Когда Джоана Буйан, сотрудница медиа-компании BuzzFeed, приехала в главный офис компании Uber (служба вызова такси) в Нью-Йорке в одной из машин сервиса, Джош Морер, генеральный директор, уже ждал ее. «Вот и вы, — сказал он, держа в руках свой iPhone, — Я следил за вами». Не самое удачное начало для интервью, темой которого среди прочего был вопрос неприкосновенности частной жизни клиентов.

Пока Буйан не напечатала свою статью в ноябре 2014 года, мало кто за пределами компании Uber вообще слышал о God View («Взгляд Бога»), программе, с помощью которой компания Uber в режиме реального времени отслеживает местонахождение тысяч водителей, заключивших с ней контракт, а также их клиентов.

Как я уже говорил, приложения запрашивают у пользователей различные разрешения, включая разрешение на передачу геолокационных данных. Приложение Uber идет еще дальше — запрашивает ваше приблизительное (Wi-Fi) и точное (GPS) местонахождение, разрешение на

получение доступа к вашим контактам, а также не позволяет мобильному устройству перейти в спящий режим (чтобы это не помешало отслеживать его перемещение).

Буйан, как утверждается, сразу же сказала Мореру, что не давала компании разрешения отслеживать ее нигде и никогда. Но на самом деле она дала это разрешение, хотя, может, и не явным образом. Разрешение было частью пользовательского соглашения, с условиями которого она согласилась, когда установила приложение на свое мобильное устройство. После интервью Морер отправил Буйан электронное письмо со списком всех ее поездок с водителями Uber за последнее время.

Компания Uber собирает досье на каждого клиента, фиксируя каждую поездку. Это плохая идея, если база данных недостаточно защищена. База данных Uber — это «золотое дно» для всевозможных шпионов, начиная с правительства США и заканчивая китайскими хакерами.

Когда Джоана Буйан, сотрудница медиа-компании BuzzFeed, приехала в главный офис компании Uber (служба вызова такси) в Нью-Йорке в одной из машин сервиса, Джош Морер, генеральный директор, уже ждал ее. «Вот и вы, — сказал он, держа в руках свой iPhone, — Я следил за вами».

Не самое удачное начало для интервью, темой которого среди прочего был вопрос неприкосновенности частной жизни клиентов.

В 2015 году компания Uber изменила ряд условий своей политики конфиденциальности, в некоторых пунктах — в худшую для клиента сторону. Теперь компания Uber будет собирать геолокационные данные обо всех своих пользователях на территории США, — даже если приложение работает только в фоновом режиме и даже если сотовая или спутниковая связь отсутствует. Как утверждает Uber, отслеживание пользователей, не находящихся на связи, происходит с помощью сетей Wi-Fi и IP-адреса. Это значит, что приложение Uber — это своего рода тихий шпион на вашем мобильном устройстве. Однако компания так и не объяснила, зачем ей это нужно.

Также компания Uber не смогла объяснить, зачем ей нужна программа God View. С другой стороны, согласно политике конфиденциальности: «Политика Uber решительно запрещает всем сотрудникам любого уровня просматривать данные водителей и пассажиров. Эта политика не распространяется только на ограниченный круг добросовестных коммерческих задач». К добросовестным коммерческим задачам относится отслеживание профилей возможных мошенников и улаживание трудностей, возникающих у водителей (например, несостоявшаяся поездка). Вероятно, в этот список не входит отслеживание перемещений журналистов.

Думаете, Uber оставляет за пользователями право удалить данные об отслеживании? Нет. И угадайте, что произойдет, если, прочитав все это, вы удалите приложение? Ваши данные все равно останутся в базе Uber.

После обновления политики конфиденциальности компания Uber также стала собирать информацию о ваших контактах. Если у вас iPhone, можно изменить настройки конфиденциальности для контактов из адресной книги. Если у вас устройство под управлением операционной системы Android, так сделать не получится.

Представители сервиса Uber заявили, что компания в настоящий момент не собирает такого рода данные о пользователях. Однако, включив сбор данных в политику конфиденциальности, с условиями которой существующие пользователи уже согласились, а новым придется это сделать, компания обеспечила себе возможность активировать соответствующие функции в любой момент. А пользователям остается только смириться с этим.

Самого факта существования программы God View в сервисе Uber уже достаточно для того, чтобы с ностальгией вспомнить о старом добром обычном такси. Раньше мы просто ловили такси, говорили адрес и расплачивались наличными по прибытии на место. Иначе говоря, поездка была практически полностью анонимной.

В начале XXI века, когда банковские карты используются практически везде, множество повседневных транзакций перешли в цифровую плоскость и стали отслеживаемыми, поэтому, вероятно, теперь существует журнал всех ваших поездок на такси — пусть даже эта информация не привязана к какому-то конкретному водителю или службе такси, но уж точно привязана к организации, выпустившей вашу банковскую карту. В 1990-х, когда я работал частным сыщиком, мне удалось отследить перемещения объекта с помощью данных об операциях по его банковской карте. Достаточно просто взглянуть на банковскую выписку, чтобы узнать, что на прошлой неделе вы пользовались услугой такси в Нью-Йорке, за которую заплатили 54 доллара.

Начиная примерно с 2010 года, службы такси применяют в своей работе данные геолокации. Теперь компания знает, где вы сели в такси и куда ехали, сколько заплатили за поездку, а также какой банковской картой расплачивались. Эта информация в соответствии с концепцией открытых

данных, разделяемой муниципальными властями Нью-Йорка, Сан-Франциско и других городов, выкладывается в общий доступ, обеспечивая исследователей богатой и анонимной базой данных. Раз имена пассажиров не указываются, разве могут подобные вещи кому-то навредить?

В 2013 году Энтони Токар, на тот момент магистрант Северо-Западного университета и стажер в компании под названием Neustar, из любопытства стал просматривать анонимные метаданные, выложенные в открытый доступ компанией NYC Taxi and Limousine Commission. В этих данных были указаны каждая поездка на машине из автопарка компании за последние годы, а также номер каждой машины, время начала и завершения поездки, адреса, стоимость и чаевые, а также права и номер лицензии таксиста (в хешированном виде). Сами по себе эти данные не представляют особого интереса. К сожалению, в данном случае хеш-функция довольно легко поддается обратному преобразованию.

Однако если объединить открытую базу данных с другими базами, пазл начинает складываться. В данном случае Токар сумел определить, в каких точках Нью-Йорка садились в такси некоторые знаменитости, например, Брэдли Купер и Джессика Альба. Как ему это удалось?

У него уже были геолокационные данные, поэтому Токар знал, откуда и куда таксисты перевозили пассажиров, но ему необходимо было выяснить, кто находился в этих машинах. Поэтому он сопоставил данные, предоставленные компанией New York Taxi and Limousine Commission, с выложенными в Интернет фотографиями из таблоидов. С базой данных папарацци.

Только подумайте об этом. Папарацци часто фотографируют знаменитостей, как раз когда они садятся или выходят из нью-йоркских такси. Часто на этих снимках хорошо виден медальон (номер лицензии) такси. Он расположен на каждой машине сбоку. По номеру такси, на фоне которого сфотографирован, скажем, Брэдли Купер, в открытых данных можно найти, откуда и куда он ехал, стоимость поездки и размер чаевых.

К счастью, не за каждым из нас следят папарацци. Но это не значит, что нет других способов отследить наши перемещения. Возможно, вы вообще не ездите на такси. Как еще узнать ваше местонахождение? Это вполне возможно. Даже если вы пользуетесь общественным транспортом.

Если вы добираетесь до работы на автобусе, поезде или пароме, о невидимости речь тоже не идет. Транспортные системы пытаются с помощью специальных мобильных приложений и технологии NFC (англ. Near Field Communications — «коммуникация ближнего поля») идентифицировать пассажиров на входе и выходе из общественного транспорта. NFC представляет собой технологию высокочастотной беспроводной связи короткого радиуса действия. Технология NFC лежит в основе ряда платежных систем, например, Apple Pay, Android Pay и Samsung Pay, благодаря которым оплата проезда наличной мелочью постепенно становится пережитком прошлого.

Представим себе, что ваш смартфон поддерживает NFC и вы установили на него специальное приложение для оплаты проезда в местном общественном транспорте. Приложение запросит привязать его к банковскому счету или банковской карте, чтобы вы всегда могли сесть на любой автобус, поезд или паром, не беспокоясь о том, что у вас вдруг не окажется наличных денег. Привязанная банковская карта, если, конечно, ее номер не скрыт специальным кодом-заменителем, может помочь транспортной компании установить вашу личность. Замена номера банковской карты зашифрованным кодом — это новая опция, предлагаемая компаниями Apple, Android и Samsung. Таким образом, у продавца (в данном случае у транспортной компании) вместо номера вашей банковской карты окажется только криптограмма. Благодаря этому в ближайшем будущем снизится риск утечки данных, поскольку преступникам будут нужны две базы данных: кодов и настоящих номеров банковских карт, им соответствующих.

Предположим, что ваш смартфон не оборудован NFC. Вместо этого вы пользуетесь персональной транспортной картой (например, социальной). У этих карт также есть только специальный номер, на который записывается или определенное число поездок на городском транспорте, или неограниченное число поездок, но в течение ограниченного времени. У самой карты есть только ее номер, который не связан с вашими персональными данными, но и в этом случае они не обязательно застрахованы от утечки. Некоторые транспортные компании требуют онлайн-регистрации, чтобы можно было отправить электронное письмо и тому подобное, следовательно, всю эту информацию можно украсть. Как бы то ни было, возможность анонимно проехаться на автобусе постепенно исчезает, единственный шанс хоть как-то этому противодействовать — платить наличными, а не персональной картой.

Эта разработка является невероятным подспорьем для полиции. Поскольку выпуском транспортных карт занимаются частные компании, а не государственные органы, они могут устанавливать любые правила, касающиеся передачи данных правоохранителям. И не только им, а даже юристам по гражданским делам — вдруг ваша бывшая супруга или супруг решит с вами за что-то поквитаться.

Поэтому любой человек, получивший доступ к журналам транспортной компании, сможет точно узнать, кто вошел в метро на такой-то станции в такое-то время — но не узнает, на какой поезд сел

этот пассажир, особенно если станция пересадочная. Что, если информацию о том, на какой поезд вы сели и куда поехали, можно было бы получить через ваше мобильное устройство?

Ученые из Нанкинского университета в Китае задались целью ответить на этот вопрос и обратили свое внимание на один из компонентов смартфонов — акселерометр. Каждое мобильное устройство оснащено этим прибором. Это крошечный чип, отвечающий за определение угла наклона вашего устройства — того, как вы его повернули, горизонтально или вертикально. Эти датчики настолько чувствительны, что ученые решили попробовать получить информацию о перемещениях человека в метро с помощью данных акселерометра. Как ни удивительно, китайским исследователям удалось с помощью данных акселерометра точно определить, каким поездом поехал определенный пассажир метро. Это связано с тем, что у большинства подземных линий есть повороты, которые влияют на акселерометр. Также важную информацию несут временные промежутки между остановками поезда — достаточно просто взглянуть на карту метро, чтобы понять, почему это так важно. Чем больше станций проехал человек, тем с большей точностью можно определить направление его движения. Ученые утверждают, что с помощью этого метода им удавалось получать достоверный результат в 92 процентах случаев.

Представим, что у вас есть старенькая машина, на которой вы добираетесь до работы. Возможно, вы считаете себя невидимым, одна машина из миллиона в потоке машин. И не исключено, что вы правы. Но новейшие технологии — они могут не иметь никакого отношения к самому автомобилю — лишают вас этой анонимности. Существует вероятность, что, приложив некоторые усилия, вас довольно быстро сможет вычислить, например, человек из машины, промчавшейся мимо вас на шоссе.

Представим, что у вас есть старенькая машина, на которой вы добираетесь до работы. Возможно, вы считаете себя невидимым, одна машина из миллиона в потоке машин. И не исключено, что вы правы. Но новейшие технологии — они могут не иметь никакого отношения к самому автомобилю — лишают вас этой анонимности.

Управление дорожного хозяйства и транспорта города Сан-Франциско начало применять систему автодорожных сборов под названием FasTrak, с помощью которой можно легко оплатить проезд через любой из восьми мостов в окрестностях Сан-Франциско и отслеживать передвижения по городу всех машин, подключенных к ней. Сканеры на платных мостах считывают информацию с установленного в машине устройства FasTrak (или EZ Pass). С этих же устройств власти Сан-Франциско стали считывать информацию о перемещениях пользователей по городу. Но чиновникам не всегда интересны ваши перемещения: скорее, им интересны парковочные места, большинство из которых оборудованы счетчиками. В тех районах, где в данный момент наблюдается высокий спрос на парковку, цены на стоянку могут возрасти. Муниципальные власти могут дистанционно регулировать цену на определенных счетчиках — например, на расположенных рядом с местом проведения массового мероприятия.

Кроме того, начиная с 2014 года, на мосту Золотые Ворота нет кассиров, принимающих плату за проезд, поэтому каждый человек, даже турист, должен производить оплату в электронном виде. Или как вариант — счет по почте. Откуда власти знают, по какому адресу высылать счет? Когда вы проезжаете пункт оплаты, ваш номерной знак фотографируют. Эти фотографии с номерными знаками также часто применяются для того, чтобы прижать любителей проскочить на красный сигнал светофора на сложном перекрестке. И все чаще полицейские прибегают к этой же стратегии, замечая плохо припаркованную машину на стоянке или придомовой территории.

Полиция в пассивном режиме отслеживает ежедневные перемещения вашей машины с помощью технологии автоматического распознавания номерных знаков (ALPR, от англ. automated license plate reading). Фотографии с номерными знаками вашей машины могут храниться вплоть до нескольких лет, в зависимости от полицейского участка. Независимо от того, зарегистрирована ли машина на имя преступника или нет, камеры ALPR сканируют и считывают каждый номерной знак, попавшийся им на пути.

Со стороны кажется, что технология ALPR нужна в первую очередь для розыска угнанных автомобилей, преступников в бегах и похищенных детей. Выглядит это следующим образом: на крыше патрульной машины закреплены три камеры, подключенные к компьютерному монитору внутри салона. Система передает данные в базу Министерства юстиции, где хранится информация о номерах угнанных машин и автомобилей, замешанных в преступлениях. Офицер полиции управляет машиной, а конструкция с камерами ALPR может заснять до 60 номерных знаков в секунду. Если номер на снимке совпадает с номером из базы данных Министерства юстиции, полицейский слышит (и видит) специальный сигнал.

Издание Wall Street Journal впервые опубликовало материал о технологии распознавания номерных знаков в 2012 году. У тех, кто выступает против технологии ALPR или просто ей не доверяет, беспокойство вызывает не столько она сама, сколько срок хранения данных и то, почему некоторые органы правопорядка не сообщают даже самим владельцам, что машины находятся под наблюдением. Это неприятный инструмент, с помощью которого полиция может выяснить, где вы

были.

«Автоматическое распознавание номерных знаков — это хитроумный способ отслеживания местонахождения водителя, а когда с течением времени данные накапливаются, можно составить подробную картину жизни человека», — отмечает Беннетт Стейн из Американского союза защиты гражданских свобод.

Некий житель Калифорнии запросил доступ к общественным архивам и был поражен количеством фотографий с его номерным знаком (более 100 штук). Большинство из них были сделаны во время переездов через мост и в других общественных местах. Однако на одной из фотографий он увидел себя и своих дочерей, выходящих из машины на дорожке у собственного дома. Прошу заметить, что этого человека не подозревали в совершении какого-нибудь преступления. Согласно документам, попавшим в руки Американского союза защиты гражданских свобод опять же из общественных архивов, даже Офис генерального юрисконсульта ФБР заинтересовался правомочностью применения технологии ALPR в отсутствие какой-либо согласованной правительственной программы.

К сожалению, для доступа к некоторым данным ALPR не требуется оформлять официальный запрос. По информации Фонда электронных рубежей, снимки с сотни с лишним камер ALPR находятся в Интернете в открытом доступе. Вам нужен только браузер. Прежде чем обнародовать результаты своего исследования, Фонд электронных рубежей обратился в каждый правоохранительный отдел, чтобы сотрудники устранили утечку данных. В Фонде заявили, что эта ошибка в настройках была обнаружена не только в этих ста случаях и, когда она вскрылась, правоохранительные органы осознали необходимость прекратить или ограничить публикацию данных в Интернете. Однако на момент написания данной книги по-прежнему можно получить доступ к изображениям номерных знаков во многих регионах, введя верный поисковый запрос в специальное поле. Одному интересующемуся удалось найти в Интернете свыше 64 000 фотографий номерных знаков вкупе с соответствующими данными о местонахождении машин за период в одну неделю.

Представим себе, что у вас нет машины и вы иногда берете ее напрокат. Конечно же, вы не невидимы, учитывая, сколько информации о себе нужно предоставить, чтобы арендовать машину — персональные данные и реквизиты банковской карты. Более того, у большинства сдаваемых напрокат машин в наши дни есть встроенный модуль спутниковой навигации. Я это знаю. Я убедился в этом на собственном опыте.

Когда вы берете машину в аренду на то время, пока ваша находится в сервисе, по условиям договора, как правило, вы не можете выезжать на ней за пределы штата. Прокатные конторы не хотят, чтобы машина покидала штат, в котором ее арендовали. Это правило в основном связано с их страховкой, а не вашей.

Со мной произошла такая история. Я привез свою машину в салон Lexus в Лас-Вегасе на ремонт, а мне на время дали прокатную машину. Поскольку салон уже закрывался и меня поторапливал сотрудник, я просто подписал договор, не читая его. Позже я на этой машине поехал в северную Калифорнию, в область залива Сан-Франциско, где у меня должно было состояться выступление. Мне позвонили из сервисного центра, чтобы обсудить технические вопросы по обслуживанию машины, а затем звонивший задал мне вопрос: «Где вы сейчас находитесь?» Я сказал, что в Калифорнии, в Сан-Рамоне. Он ответил: «Да, мы вас видим». Затем он отчитал меня за то, что я вывез машину из штата. Судя по всему, в договоре, который я подписал не глядя, содержался пункт о том, что на машине нельзя выезжать за пределы штата Невада.

Когда вы арендуете или одалживаете чужую машину, возникает соблазн подключить к мультимедийной системе автомобиля свое устройство, чтобы воссоздать в машине тот комфорт, к которому вы привыкли дома. Разумеется, тут же возникают проблемы приватности. Это не ваша машина. Что случится с данными информационно-развлекательной системы, когда вы вернете машину обратно?

Когда вы арендуете или одалживаете чужую машину, возникает соблазн подключить к мультимедийной системе автомобиля свое устройство, чтобы воссоздать в машине тот комфорт, к которому вы привыкли дома. Разумеется, тут же возникают проблемы приватности. Это не ваша машина. Что случится с данными информационно-развлекательной системы, когда вы вернете машину обратно?

Перед подключением своего устройства к чужой машине внимательно изучите мультимедийную систему. Вполне возможно, подключая смартфон через интерфейс Bluetooth, на экране в машине вы увидите список устройств или имен предыдущих пользователей. Подумайте, хотите ли вы быть в этом списке.

Другими словами, ваши данные не исчезнут, когда вы сдадите машину. Вам придется удалять их самостоятельно.

Вы можете подумать, что дурного, если другие люди узнают о ваших музыкальных предпочтениях? Проблема в том, что в этом случае вы предоставите доступ не только к своей музыке. При подключении большинства мобильных устройств к мультимедийной системе автомобиля также открывается доступ к списку ваших контактов. Предполагается, что, если вы за рулем захотите позвонить кому-то в режиме hands-free, хранящиеся в памяти автомобиля данные из вашего списка контактов станут дополнительным удобством. Проблема заключается в том, что это не ваша машина.

«Когда я беру напрокат машину, — говорит Дэвид Миллер, руководитель отдела безопасности компании Covisint, — я ни за что не подключу к ней свой телефон. Она загрузит к себе все мои контакты, потому что так запрограммирована. В большинстве арендованных машин можно просмотреть чужие контакты (если кто-то подключал свое устройство до вас)».

То же самое происходит и при продаже автомобиля. Новые модели машин более активно вовлечены в вашу цифровую деятельность. Хотите проверить Twitter? Хотите выложить пост на Facebook? Современные машины все больше и больше напоминают компьютеры и сотовые телефоны. Прежде чем продать машину, необходимо удалить из нее все персональные данные.

Работа в сфере безопасности приучает обдумывать наперед даже самые рутинные операции. «Сначала я активно включаю свою машину в свою жизнь, — говорит Миллер, — а затем через пять лет я ее продаю. Как мне отсоединить ее от всей моей жизни? Я не хочу, чтобы покупатель [машины] смог увидеть список моих друзей на Facebook, поэтому нужно уничтожать данные. Люди, для которых важна безопасность, уделяют больше внимания уязвимостям, связанным с удалением данных, чем с их предоставлением».

Как и в случае с мобильным устройством, нужно защищать свою машину паролем. Но тут вам не удастся просто запаролить мультимедийную систему (по крайней мере, так было на момент написания данной книги). И не удастся просто взять и удалить все аккаунты, которые вы подключали к своей машине — тут ваши возможности зависят от производителя, марки и модели автомобиля. Возможно, ситуация изменится — может быть, кто-то изобретет универсальную кнопку, с помощью которой можно удалить из вашей машины сразу все свои персональные данные. А до тех пор хотя бы выйдите в Интернет и смените все пароли в своих социальных сетях после продажи машины.

Вероятно, лучшим примером компьютера на колесах является Tesla, электромобиль, который достоин считаться произведением искусства. В июне 2015 года компания Tesla пробила важный порог: автомобили Tesla по всему миру в совокупности проехали более одного миллиарда миль.

У меня Tesla. Это отличные машины, но их приборная доска словно взята из рубки управления космического корабля, а к сотовой сети они подключены постоянно, поэтому естественным образом возникает вопрос о том, какие данные они собирают.

Когда вы покупаете электромобиль Tesla, вы подписываете соглашение. Вы можете регулировать, будет ли Tesla фиксировать какую-либо информацию о вашей машине с помощью беспроводной системы связи. Вы можете подключать или отключать обмен данными с серверами Tesla через сенсорный экран на приборной панели. Многие люди соглашаются, что их данные помогут компании Tesla развиваться и совершенствовать свои автомобили.

Как заявляет компания Tesla в своей политике конфиденциальности, компания может собирать данные об идентификационном номере транспортного средства (VIN), скорости, показаниях одометра, расходе заряда аккумулятора, истории его зарядки, работе электрооборудования, программном обеспечении, мультимедийной системе, безопасности (включая информацию о системе пассивной безопасности, тормозах, стояночном тормозе) и прочие данные, необходимые для диагностики и анализа состояния транспортного средства. Компания Tesla утверждает, что может получать эту информацию лично (например, во время техобслуживания) или удаленно.

Так написано в их политике конфиденциальности.

В действительности же компания также может определять местонахождение и статус вашей машины в любой момент времени. Что касается общения с журналистами, компания Tesla неохотно распространяется о том, какие данные и каким образом она собирает и как их использует. Как и Uber, Tesla заняла положение Господа Бога, которому известно абсолютно все о каждой своей машине в каждый момент времени.

Если вам от этого неуютно, можно связаться с компанией Tesla и выйти из программы обмена данными. Однако в таком случае вы откажетесь и от автоматического обновления программного обеспечения, а вместе с ним и от устранения проблем безопасности и обновления функциональных возможностей.

Разумеется, сообществу специалистов по информационной безопасности интересно все, что связано

с автомобилями Tesla, и независимый исследователь Нитеш Данжани выявил несколько проблем. Хотя Данжани согласен со мной в том, что Tesla Model S — это отличная машина и фантастический продукт новых технологий, он обнаружил, что компания Telsa для удаленного доступа к системам автомобиля применяет очень слабую однофакторную аутентификацию. На веб-сайте и в приложении Tesla отсутствует возможность ограничить количество попыток входа в учетную запись, а значит, хакер может подобрать пароль от аккаунта методом перебора. Получается, что кто-то посторонний (взломавший ваш пароль) может войти и через программный интерфейс Tesla посмотреть, где находится ваше транспортное средство. Также он может удаленно авторизоваться в приложении Tesla и перехватить контроль над системами автомобиля — кондиционером, светом и пр., хотя автомобиль при этом должен быть неподвижным. Большинство моментов, которые беспокоили Данжани, компания Tesla успела устранить к моменту написания данной книги, но это пример того, как много производителям автомобилей надо сделать, чтобы защитить свои машины в наши дни. Нельзя просто разработать приложение для удаленного запуска двигателя и проверки состояния автомобиля. Оно также должно быть хорошо защищено. Новейшая опция, которая называется Summon, позволяет отправить автомобилю команду, чтобы тот самостоятельно выехал из гаража или с парковки. В будущем с помощью этой функции машина сможет сама забирать вас из любой точки в стране. Как в старом сериале «Рыцарь дорог».

Пытаясь ответить на критику в газете New York Times, компания Tesla согласилась с тем, что собираемые ею сведения обладают мощным потенциалом. Джон Бродер из Times сообщил, что его автомобиль Tesla S вышел из строя и создал ему массу затруднений. Компания Tesla парировала, что в истории Бродера масса неувязок. Например, Бродер двигался со скоростью 104–130 км/ч, а средняя температура в салоне составляла 22 °C. Согласно изданию Forbes, «в данных бортового журнала автомобиля Model S указана выставленная температура в салоне, уровень заряда аккумулятора в течение всей поездки, скорость передвижения машины в каждую минуту времени и точный маршрут следования — вплоть до того факта, что водитель ездил кругами по парковке до тех пор, пока аккумулятор не разрядился практически полностью».

Телематика — это логичное продолжение идеи бортовых самописцев, обязательных к установке на всех автомобилях, произведенных для продажи на территории США, начиная с 2015 года. Но бортовые самописцы в машинах — это отнюдь не новшество. Впервые необходимость в подобных устройствах возникла в 1970-х годах с появлением первых подушек безопасности. В случае ДТП в те времена люди часто получали смертельно опасные травмы именно из-за самих подушек, а некоторые даже умирали в результате удара, нанесенного им подушкой. В некоторых случаях, если бы машина не была оснащена этими подушками, люди могли бы выжить. Чтобы доработать средство защиты, инженерам нужны были данные о поведении подушек безопасности за несколько секунд до и после аварии. Для получения этих данных подушки оснастили модулями датчиков и диагностики (SDM). Однако владельцам автомобилей до недавних пор не сообщали о том, что эти датчики записывают данные, связанные с их вождением.

Бортовые самописцы в автомобилях (так же, как и в самолетах) фиксируют внезапные перегрузки и записывают только несколько секунд до и после такого события, например, внезапное ускорение, поворот и резкое торможение.

Но вполне можно предположить, что подобных данных собирается все больше и больше как бортовыми самописцами, так и в режиме реального времени, через подключение к сотовой сети. Представьте себе, что в будущем в памяти автомобиля или в «облаке» можно будет хранить данные за три-пять дней. Вместо того чтобы пытаться описать тот странный свистящий звук, который вы слышите, когда машина превышает скорость 55 км/ч, вы сможете предоставить своему механику доступ к записанным данным. Но главный вопрос заключается в том, у кого он будет в принципе? Даже компания Tesla признает, что собранные данные могут попасть в руки третьим лицам.

А что, если третьей стороной окажется ваш банк? Представим себе, что он заключил соглашение с производителем вашего автомобиля, чтобы оценить вашу манеру вождения и в соответствии этим предложить вам индивидуальные условия автокредитования в будущем. Или компания, занимающаяся страхованием жизни и здоровья. Или даже компания по автострахованию. Возможно, правительство должно отрегулировать вопрос о том, кто получает данные о вашем транспортном средстве и как вы можете защитить неприкосновенность своих данных.

В настоящий момент вы мало что можете сделать, но определенно стоит обратить на это внимание в будущем.

Даже если у вас не Tesla, для вашего автомобиля может существовать приложение, позволяющее открывать двери, запускать двигатель или даже проводить диагностику определенных систем машины. Один исследователь продемонстрировал, что эти сигналы — между машиной, «облаком» и приложением — можно перехватить и с их помощью отследить определенную машину, свободно ее открыть, привести в действие клаксон, сигнализацию и даже запустить двигатель. Хакер может сделать практически все, за исключением переключения передачи и угона машины. Для этого все еще нужен ключ зажигания. Хотя я недавно выяснил, как отключить брелок-контроллер от автомобиля Tesla, полностью обездвижив машину. С помощью небольшого передатчика с рабочей

частотой 315 МГц можно сделать так, чтобы брелок-контроллер невозможно было засечь, т. е. машина будет полностью отключена.

Даже если у вас не Tesla, для вашего автомобиля может существовать приложение, позволяющее открывать двери, запускать двигатель или даже проводить диагностику определенных систем машины. Один исследователь продемонстрировал, что эти сигналы — между машиной, «облаком» и приложением — можно перехватить и с их помощью отследить определенную машину, свободно ее открыть, привести в действие клаксон, сигнализацию и даже запустить двигатель. Хакер может сделать практически все, за исключением переключения передачи и угона машины.

Во время своего выступления на конференции DEF CON23 Сэми Камкар, специалист по безопасности, известный как автор червя Samy для MySpace в 2005 году, продемонстрировал разработанное им устройство под названием OwnStar, которое способно перехватывать и имитировать сигнал системы OnStar. С помощью этого устройства он может открыть автомобиль General Motors, подключенный к OnStar. Для этого необходимо прикрепить устройство на бампер или днище кузова машины. Устройство имитирует сигнал точки доступа OnStar, к которой автоматически подключается мобильное устройство ничего не подозревающего водителя (разумеется, если водитель ранее подключался к настоящей точке доступа). Как только пользователь запускает мобильное приложение OnStar в операционной системе Android или iOS, код OwnStar использует уязвимость в приложении для перехвата учетных данных водителя. «В тот момент, когда вы оказались в моей сети и открыли приложение, контроль перешел в мои руки», — сказал Камкар.

Услышав звуковой сигнал и получив учетные данные для входа в интерфейс RemoteLink (приложение OnStar), хакер может найти машину на переполненной парковке, открыть ее и украсть из нее любые ценные предметы. Затем злоумышленник снимет устройство с бампера. Это очень аккуратный метод взлома, поскольку не остается никаких следов. Владельцу — и страховой компании — остается только ломать голову, что произошло.

Специалисты обнаружили уязвимость системы беспроводной связи между автомобилями, разработанной для регулирования трафика. Машины, объединенные в систему автомобиль-автомобиль (V2V) и автомобиль-инфраструктура (V2I), вместе известные как система V2X (vehicle to everything, автомобиль-все), обмениваются данными друг с другом по десять раз в секунду, используя для этого технологию 802.11p — Wi-Fi-соединение с частотным диапазоном 5,9 ГГц.

К сожалению, эти данные передаются в незашифрованном виде — по-другому никак. Когда машины мчатся по трассе, задержка в одну миллисекунду (именно столько времени уходит на дешифрование сигнала) может привести к столкновению, поэтому разработчики остановились на открытом, незашифрованном способе связи. Зная это, они настояли на том, чтобы в пересылаемых данных не содержалось никаких личных сведений, даже номера автомобиля. Однако чтобы избежать ложных сигналов, в каждом сообщении присутствует цифровая подпись. Именно по этим цифровым подписям, напоминающим идентификатор IMEI (серийный номер мобильного телефона), транслируемый сотовым телефоном, можно отследить владельца транспортного средства.

Джонатан Петит, один из авторов этого исследования, рассказал изданию Wired.com: «Транспортное средство говорит: “Я Элис, вот где я нахожусь, вот какая у меня скорость и направление движения”. Все вокруг могут это услышать… Они могут сказать: “Там Элис, она сказала, что была дома, но заехала в аптеку, а затем в женскую консультацию”, — как-то так… Кто угодно может узнать много личного о пассажире».

Петит разработал систему ценой около 100 долл., с помощью которой можно перехватывать данные, передаваемые в сети V2X. По его подсчетам, небольшой город можно полностью оснастить подобными датчиками примерно за 1 млн долл. Вместо того чтобы тратить бюджет на содержание многочисленной полиции, лучше применять подобные датчики, которые позволят идентифицировать водителей и, что важнее, выяснить их привычки.

Национальное управление безопасностью движения на трассах США и европейские инстанции предложили каждые пять минут менять метку автомобиля, передаваемую по беспроводным каналам связи, то есть его «псевдоним». Однако это не остановит настойчивого хакера, который просто установит вдоль дороги больше датчиков для идентификации автомобиля до и после смены метки. Проще говоря, воспрепятствовать идентификации транспортного средства очень трудно.

«Смена псевдонима не остановит слежку. Она может только слегка ее ослабить, — говорит Петит. — Но в любом случае необходимо работать над конфиденциальностью. Мы хотим продемонстрировать, что в каждой среде у вас должна быть эта защита, иначе кто-нибудь сможет следить за вами».

Возможность подключения автомобилей к Интернету — это преимущество для владельцев машин, а производители могут при необходимости молниеносно выпускать исправленные версии программного обеспечения. На момент написания данной книги у машин марок Volkswagen, Land

Rover и Chrysler были обнаружены большие проблемы с безопасностью программного обеспечения. Однако только несколько производителей, в их числе Mercedes, Tesla и Ford, обновляют программное обеспечение своих автомобилей дистанционно, по беспроводной связи. Остальные должны обращаться в автосалон.

Если вас пугает то, что Tesla и Uber отслеживают каждую вашу поездку, то автомобили с автопилотом напугают еще сильнее. Как и устройства персональной слежки, которые мы носим в своих карманах — сотовые телефоны, — автомобили, способные передвигаться самостоятельно, должны будут вести учет тех мест, куда мы собираемся ехать, и, возможно, быть в курсе того, где мы находимся в данный момент, чтобы всегда быть наготове. По версии Google и других сервисов, в городах больше не нужны будут парковки — машина будет колесить по району, пока вам не понадобится. Также, возможно, получит распространение модель поведения, при которой у людей не будет в собственности машин, а они при необходимости будут пользоваться любой из них, оказавшейся поблизости.

Как и сотовые телефоны, которые в большей степени являются компьютерами, чем телефонами в традиционном смысле слова, беспилотные машины так же станут новым видом компьютерной техники. Они будут представлять собой автономные вычислительные системы и, даже если их отрежут от Интернета, смогут мгновенно и самостоятельно принимать решения на дороге. С помощью сотового соединения они будут подключены к различным облачным сервисам, благодаря которым будут в режиме реального времени получать информацию о ситуации на дороге, дорожно-ремонтных работах и погодных условиях от Национальной метеорологической службы США.

Эти новые функции в настоящий момент присутствуют в ряде обычных, не беспилотных автомобилей. Но, по прогнозам, уже к 2025 году большинство машин на дорогах будут подключены к другим машинам, к дорожным службам и, вероятно, большой процент этих машин составят беспилотные. Представьте себе, к чему может привести уязвимость в программном обеспечении такой машины.

При этом каждая ваша поездка будет где-то фиксироваться. Вам нужно будет приложение, что-то наподобие современного Uber, которое будет подключено к вам и к вашему мобильному устройству. Это приложение будет записывать каждую поездку и, вероятно, связанные с ней расходы, если вы будете расплачиваться прикрепленной банковской картой, номер которой могут потребовать, если не у компании Uber, то у вашего банка. Принимая во внимание то, что в разработке и обслуживании соответствующего программного обеспечения, скорее всего, будет принимать участие какая-нибудь негосударственная фирма, вам придется полагаться на милость этой компании, которая будет решать, делиться вашими персональными данными с правоохранительными органами или нет.

Добро пожаловать в будущее.

Надеюсь, что к тому моменту, когда вы будете это читать, к производителям подключенных к сети автомобилей и их стандартам связи будут предъявляться более жесткие требования — или хотя бы появится шанс, что такие требования будут введены в ближайшем будущем. Вместо того чтобы активно применять широко распространенные технологии безопасности программного обеспечения и аппаратных средств, которые сегодня уже являются стандартом, автомобильная промышленность, как, впрочем, и медико-техническая и другие промышленности, пытается изобрести колесо — как будто за последние сорок лет не было проведено множество исследований в области информационной безопасности. Было, и лучше бы представители указанных сфер начали следовать существующим практикам вместо того, чтобы утверждать, что делают нечто кардинально новое. Не новое. К сожалению, взлом автомобиля может привести к гораздо более серьезным последствиям, чем простой вирус на компьютере и синий экран смерти. В случае с автомобилем может погибнуть или получить травмы человек. На момент написания данной книги как минимум один человек погиб в машине Tesla, пока та двигалась в режиме автопилота — предстоит выяснить, в чем заключалась проблема: в неисправных тормозах или в том, что программа приняла ошибочное решение.

Прочитав это, вы, возможно, не захотите выходить из дома. В следующей главе мы поговорим о том, как гаджеты в нашем доме способствуют записи и прослушке всего, что происходит за закрытыми дверями. И вовсе не государственных органов мы должны опасаться в первую очередь.

Глава 12

СЛЕЖКА ЧЕРЕЗ ИНТЕРНЕТ

Несколько лет назад никто не думал о термостате в вашем доме. Это был простой управляемый вручную термостат, позволяющий поддерживать в доме комфортную температуру. Позднее термостаты стали программируемыми. А затем компания Nest решила, что у вас должна быть возможность управлять программируемым термостатом с помощью веб-приложения. Вы понимаете, к чему я веду, не так ли?

В одном язвительном обзоре «умного» термостата Honeywell Wi-Fi Smart Touchscreen Thermostat на сайте магазина Amazon пользователь под ником «General» написал, что его бывшая жена забрала у него дом, собаку и значительную часть пенсионных накоплений, но у него остался пароль от термостата Honeywell. Этот пользователь утверждает, что поднимает температуру в доме, пока бывшая жена и ее новый любовник за городом, а затем опускает ее до нормы перед их возвращением. «Могу себе представить, какие счета за электричество они получают. При мысли об этом я улыбаюсь».

Исследователи, участвующие в конференции Black Hat USA 2014 для специалистов в области информационной безопасности, выявили несколько способов, с помощью которых прошивка термостата Nest может быть скомпрометирована. Следует отметить, что многие из этих способов требуют наличия физического доступа к устройству, то есть кто-то должен войти в ваш дом и подключиться к USB-интерфейсу термостата. Дэниел Буентелло, независимый исследователь в области безопасности, один из четырех докладчиков, чье выступление было посвящено вопросам взлома этого устройства, сказал: «Это компьютер, на который пользователь не может установить антивирус. Хуже того, существует тайная лазейка, которую мог бы использовать злоумышленник. Фактически этот прибор может использоваться в качестве устройства слежения».

Исследователи продемонстрировали видео, в котором было видно, как они изменили интерфейс термостата Nest (сделали его похожим на объектив типа «рыбий глаз», использованный в компьютере HAL 9000) и оснастили его дополнительными функциями. Интересно то, что исследователи не смогли отключить в устройстве функцию автоматической передачи данных, поэтому они создали для этого собственный инструмент. Этот инструмент должен был блокировать поток данных в Google, родительскую компанию Nest.

Комментируя эту презентацию, Зоз Куччиас из компании Nest позднее рассказала ресурсу Venture Beat: «Все аппаратные устройства, от ноутбуков до смартфонов, подвержены взлому; эта проблема не уникальна. Речь идет о физическом взломе, требующем физического доступа к самообучающемуся термостату Nest. Если бы злоумышленник сумел попасть в ваш дом, скорее всего, он выбирал бы между установкой собственного устройства и кражей драгоценностей. Такой взлом не ставит под угрозу безопасность наших серверов или соединений с ними, и насколько мы знаем, ни к одному из устройств не был получен доступ, ни одно из них не было скомпрометировано. Безопасность клиентов очень важна для нас, и нашим приоритетом является уязвимость от удаленного взлома. Защититься от этой угрозы можно, купив камеру Dropcam Pro, позволяющую наблюдать за домом, пока вас там нет».

Несколько лет назад никто не думал о термостате в вашем доме. Это был простой управляемый вручную термостат, позволяющий поддерживать в доме комфортную температуру. Позднее термостаты стали программируемыми. А затем компания Nest решила, что у вас должна быть возможность управлять программируемым термостатом с помощью веб-приложения. Вы понимаете, к чему я веду, не так ли?

С приходом Интернета вещей такие компании, как Google, стремятся колонизировать некоторые его области, завладев платформами, которые будут использовать многие другие продукты. Иначе говоря, эти компании хотят, чтобы устройства, созданные другими производителями, подключались именно к их сервисам, а не к каким-то другим. Компании Google принадлежит как DropCam, так и Nest, однако она хочет, чтобы к вашему аккаунту Google были подключены и многие другие устройства, например, умные лампочки и радио/видеоняни. Преимущество этого, по крайней мере, для Google заключается в возможности сбора большего количества данных о ваших привычках (и это касается любой крупной компании, будь то Apple, Samsung и даже Honeywell).

Говоря об Интернете вещей, эксперт по компьютерной безопасности Брюс Шнайер заметил: «Это очень похоже на компьютерную индустрию 90-х годов. Никто не обращает внимания на безопасность, никто не загружает обновления, никто ничего не знает — это очень, очень плохо, и однажды на нас обрушатся проблемы. Злоумышленники будут использовать уязвимости, которые невозможно будет устранить».

Чтобы доказать это, летом 2013 года журналистка Кашмир Хилл провела журналистское расследование, попытавшись самостоятельно взломать компьютер. Используя поисковую систему

Google, она обнаружила простую фразу, которая позволила ей управлять некоторыми домашними сетевыми концентраторами Insteon. Сетевой концентратор (или хаб) представляет собой центральное устройство, которое обеспечивает доступ к мобильному приложению или непосредственно к Интернету. Через это приложение человек может управлять освещением в своей гостиной, запирать двери дома или регулировать температуру в нем. Подключившись к Интернету, владелец может управлять всем этим, находясь, скажем, в командировке.

Как показала Хилл, злоумышленник также может использовать Интернет для получения удаленного доступа к концентратору. В качестве дополнительного доказательства она обратилась к Томасу Хэтли, совершенно незнакомому человеку из Орегона, и спросила, может ли она использовать его дом для проведения своего исследования.

Находясь в своем доме в Сан-Франциско, Хилл смогла включить и выключить освещение в доме Хэтли, находящемся в тысяче километров от нее. Она также могла бы управлять кранами в ванной, вентиляторами, телевизорами, водяными насосами, дверями гаража и камерами видеонаблюдения, если бы они были подключены к концентратору.

Проблема (в настоящее время исправленная) заключалась в том, что компания Insteon сделала всю информацию Хэтли доступной через Google. Еще хуже то, что доступ к этой информации в то время не был защищен паролем, поэтому человек, которому стало об этом известно, мог контролировать любой концентратор Insteon, обнаруженный через Интернет. Маршрутизатор Хэтли был защищен паролем, однако его можно было обойти, определив порт, который когда-то использовался системой Insteon, что и сделала Хилл.

«Дом Томаса Хэтли был одним из восьми, к которым я смогла получить доступ, — пишет Хилл. — Мне удалось обнаружить важную информацию — не только о том, какие приборы и устройства были в доме, но и о часовых поясах (а также о ближайшем крупном городе), IP-адресах и даже имени ребенка; по-видимому, родители хотели иметь возможность удаленно управлять его телевизором. По крайней мере, в трех случаях информации оказалось достаточно для того, чтобы определить реальное местонахождение дома. Имена большинства систем были стандартными, однако в одном случае имя включало название улицы, благодаря чему мне удалось найти конкретный дом в Коннектикуте».

Примерно в то же время подобная проблема была обнаружена Нитешем Данджани, исследователем по вопросам безопасности. Данджани рассматривал систему освещения Philips Hue, которая позволяет владельцу регулировать цвет и яркость лампочки с помощью своего мобильного устройства. Данная лампочка имеет диапазон из шестнадцати миллионов цветов.

Данджани обнаружил, что простого сценария, внедренного в компьютер домашней сети, было достаточно для осуществления распределенной атаки типа «отказ в обслуживании» (Distributed Denial of Service, DDoS) на систему освещения. Другими словами, он по желанию мог отключать освещение в любой комнате, в которой были установлены лампы Philips Hue. Его сценарий содержал простой код, отключающий лампочку при каждой попытке пользователя ее включить. И так продолжалось, пока этот код присутствовал на компьютере.

Данджани сказал, что это может представлять серьезные проблемы для офисного здания или многоквартирного дома. Код отключает освещение, а человек, позвонивший в местную энергетическую компанию, выясняет, что в его районе отключений электроэнергии не было.

Устройства, входящие в систему домашней автоматизации, доступ к которым осуществляется через Интернет, могут стать не просто непосредственной целью DDoS-атак, они также могут быть скомпрометированы и подключены к ботнету — армии инфицированных устройств, управляемой одним оператором, который может использовать их для осуществления DDoS-атак на другие подключенные к Интернету системы. В октябре 2016 года компания под названием Dyn, предоставляющая услугу DNS таким крупным веб-брендам, как Twitter, Reddit и Spotify, сильно пострадала от одной из таких атак. Миллионы пользователей в восточной части Соединенных Штатов не смогли получить доступ ко многим крупным сайтам из-за того, что их браузерам не удалось подключиться к DNS-сервису компании Dyn.

Причиной стала вредоносная программа под названием Mirai, сканирующая Интернет в поисках уязвимых устройств, например, камер видеонаблюдения, маршрутизаторов, видеорегистраторов и радио/видеонянь, которые можно захватить и использовать для осуществления дальнейших атак. Программа Mirai пытается получить контроль над устройством путем простого угадывания пароля. В случае успеха устройство подключается к ботнету и ожидает дальнейших инструкций. Теперь с помощью простой однострочной команды оператор ботнета может заставить сотни тысяч и даже миллионы устройств отправить данные на целевой сайт и наводнить его информацией, что в итоге приведет к его отключению.

Несмотря на то что вы не можете помешать хакерам осуществить DDoS-атаку на кого-то другого, вы можете стать невидимым для их ботнетов. Первое, что вы должны сделать перед началом

использования устройства, являющегося частью Интернета вещей, — это изменить пароль на более сложный. Если вы уже используете подобное устройство, то удалить с него любой вредоносный код можно с помощью перезагрузки.

Первое, что вы должны сделать перед началом использования устройства, являющегося частью Интернета вещей, — это изменить пароль на более сложный. Если вы уже используете подобное устройство, то удалить с него любой вредоносный код можно с помощью перезагрузки.

Компьютерные программы могут контролировать и другие системы умного дома.

Если в вашем доме есть новорожденный, у вас наверняка есть и радио/видеоняня. Это устройство, представляющее собой микрофон, камеру или их сочетание, позволяет родителям следить за своим ребенком, находясь за пределами детской комнаты. К сожалению, эти устройства могут позволить наблюдать за ребенком и посторонним.

Аналоговые радионяни использовали частоты беспроводной передачи данных в диапазоне от 43 до 50 МГц. Эти частоты были впервые использованы в 1990-х годах для беспроводных телефонов, и любой обладатель дешевого радиосканера мог легко перехватывать разговоры, причем пользователи этих беспроводных телефонов ни о чем не догадывались.

Даже сегодня хакер может применить анализатор спектра для определения частоты, используемой конкретной аналоговой радионяней, а затем использовать различные схемы демодуляции для преобразования электрического сигнала в звуковой. Также ему хватило бы полицейского сканера из магазина электроники. Было много судебных разбирательств, в которых участвовали соседи, которым использование одинаковых устройств, настроенных на одни и те же каналы, позволяло подслушивать друг друга. В 2009 году Уэс Денков из Чикаго подал в суд на производителя видеоняни Summer Infant Day & Night Baby, заявив, что его сосед может слышать личные разговоры, ведущиеся в его доме.

В качестве контрмеры вы можете использовать цифровое устройство. Подобные вещи тоже не защищены от прослушивания, однако предусматривают больше параметров конфигурации. Например, сразу после покупки вы можете обновить прошивку радио/видеоняни (программное обеспечение, записанное в микросхеме). Также не забудьте изменить имя пользователя и пароль, заданные по умолчанию.

Здесь вы снова можете столкнуться с особенностью устройства, на которую вы не в силах повлиять. Нитеш Данджани обнаружил, что беспроводная веб-няня Belkin WeMo использует в приложении токен, который, будучи установлен на мобильное устройство в домашней сети, остается активным постоянно, где бы вы ни находились. Допустим, вы зашли познакомиться со своей новорожденной племянницей и ваш брат предлагает вам загрузить на свой смартфон приложение Belkin через его домашнюю локальную сеть (хорошо, если она защищена паролем WPA2). Теперь у вашего брата есть постоянный доступ к вашему смартфону.

Данджани отметил, что этот недостаток присутствует во многих взаимосвязанных устройствах Интернета вещей. По сути, эти устройства доверяют всему, что подключено к локальной сети. Если в ближайшем времени в нашем доме действительно будет присутствовать двадцать-тридцать таких устройств, как некоторые полагают, то эта модель обеспечения безопасности должна измениться. Поскольку все устройства сети являются доверенными, то уязвимость одного из них, например, веб/радио/видеоняни, лампочки или термостата, может позволить злоумышленнику удаленно получить доступ к вашей «умной» домашней сети и предоставить ему возможность узнать о ваших привычках еще больше.

Задолго до появления мобильных приложений существовали пульты дистанционного управления. Большинство из нас слишком молоды, чтобы помнить те дни, когда в телевизорах еще не было дистанционного управления и, чтобы переключить программу, надо было вставать с дивана. Или чтобы прибавить громкость. Сегодня мы можем, сидя на диване, управлять телевизором с помощью голосовых команд. Кроме удобства это также означает, что телевизор все время находится в режиме ожидания, чтобы включиться, когда получит команду.

Задолго до появления мобильных приложений существовали пульты дистанционного управления.

Большинство из нас слишком молоды, чтобы помнить те дни, когда в телевизорах еще не было дистанционного управления и, чтобы переключить программу, надо было вставать с дивана. Или чтобы прибавить громкость. Сегодня мы можем, сидя на диване, управлять телевизором с помощью голосовых команд. Кроме удобства это также означает, что телевизор все время находится в режиме ожидания, чтобы включиться, когда получит команду.

Поначалу пульты дистанционного управления должны были находиться в прямой видимости телевизора и использовали для работы свет, а именно инфракрасный луч. Пульт дистанционного управления, работающий от батарейки, излучал последовательность световых вспышек, почти не

воспринимаемых человеческим глазом, но детектируемых приемником телевизора (отсюда важность прямой видимости). Как выключенный телевизор узнавал, что вы хотите его включить? Очень просто — инфракрасный датчик внутри телевизора был включен всегда («находился в режиме ожидания»), готовый в любой момент включить устройство целиком, получив от пульта определенную последовательность инфракрасных вспышек.

Со временем пульты дистанционного управления телевизором стали использовать радиосигналы. Это означало, что вам уже не нужно было стоять прямо перед телевизором; вы могли находиться в стороне от него, а иногда даже в другой комнате. Опять же телевизор находился в режиме ожидания, готовый к тому, чтобы включиться по первому требованию.

Вернемся к телевизорам, управляемым при помощи голоса. Для них не нужен пульт, который приходится держать в руке и который теряется в самый неподходящий момент. Вместо этого вы произносите что-нибудь вроде «Включить телевизор» или «Привет, телевизор», и телевизор волшебным образом включается.

Весной 2015 года исследователи по вопросам безопасности Кен Мунро и Дэвид Лодж захотели проверить, не подслушивают ли управляемые голосом телевизоры Samsung ведущиеся в комнате разговоры, даже находясь в выключенном состоянии. Хотя они выяснили, что цифровые телевизоры действительно ничего не делают, пока они отключены (что несколько обнадеживает), они записывают все, что говорится после произнесения простой команды вроде «Привет, телевизор» (то есть они записывают все, пока не получат команды выключиться). Кто из нас помнит о необходимости сохранять абсолютную тишину во время работы телевизора?

Мы не храним молчание, и еще больше беспокоит то, что сказанное нами (и записанное) после команды «Привет, телевизор» не шифруется. Если мне удастся подключиться к вашей домашней сети, то я смогу подслушать любой разговор, который ведется в вашем доме во время работы телевизора. Аргументом в пользу использования режима ожидания является то, что устройство ожидает получить от вас дополнительные команды, например, «Увеличить громкость», «Переключить канал» или «Отключить звук». Все бы ничего, да только захваченные голосовые команды посылаются на спутник, прежде чем будут обработаны. А поскольку поток данных не шифруется, я могу осуществить атаку посредника (Man-in-the-Middle) на ваш телевизор, по своему желанию подавая ему свои собственные команды для переключения канала, изменения уровня громкости или отключения телевизора.

Давайте на мгновение задумаемся об этом. Это означает, что если вы находитесь в комнате с телевизором, управляемым голосом, и в середине беседы с кем-то решаете включить его, то этот цифровой телевизор может записать весь ваш последующий разговор. Более того, записанная беседа о предстоящей продаже выпечки в начальной школе может быть передана на сервер, находящийся очень далеко от вашего дома. Фактически компания Samsung передает эти данные не только себе, но и другой компании под названием Nuance, занимающейся распознаванием речи. Теперь эти две компании обладают важной информацией о предстоящей продаже выпечки.

Однако давайте посмотрим правде в глаза: обычно в своей гостиной вы говорите не о продаже выпечки. Вы можете говорить о чем-то незаконном, чем могут заинтересоваться правоохранительные органы. Вполне вероятно, что эти компании будут информировать полицию, однако если правоохранительные органы уже интересуются вами, они могут получить ордер, *заставляющий* эти компании предоставить им полные стенограммы ваших разговоров. «*Очень жаль, но вас сдал ваш умный телевизор...*»

В свою защиту компания Samsung заявила, что подобное подслушивание предусмотрено соглашением о конфиденциальности, которое все пользователи неявно принимают, включая телевизор. Однако когда вы последний раз читали соглашение о конфиденциальности перед первым включением устройства? Компания Samsung заявила о том, что в ближайшем будущем все коммуникации с ее телевизорами будут зашифрованы. Тем не менее по состоянию на 2015 год большинство моделей, представленных на рынке, используют открытые каналы связи.

К счастью, существуют способы отключить эту функцию слежения на вашем телевизоре Samsung, а возможно, и на телевизорах других производителей. Для пользователей телевизоров Samsung Smart TV: перейдите в меню **Настройки —> Поддержка — > Условия и политика —> Условия распознавания голосом** (Settings —> Support —> Terms & Policy —> Voice Recognition Terms) и откажитесь от условий соглашения. Учтите, что, если вы не хотите, чтобы ваш телевизор записывал конфиденциальные разговоры в вашем доме, вам придется пожертвовать возможностью управлять им с помощью голосовых команд. При этом вы по-прежнему сможете выбрать кнопку включения микрофона на пульте дистанционного управления и произнести команду. Или встать с дивана и переключить программу самостоятельно. Я знаю. Жизнь трудна.

Проблема незашифрованных потоков данных касается не только компании Samsung. При тестировании умных телевизоров компании LG один исследователь обнаружил, что данные отправляются в LG через Интернет каждый раз, когда зритель переключает канал.

Кроме того, на этом телевизоре есть функция **Collection of watching info** (Сбор информации о просмотре), которая включена по умолчанию. Ваша «информация о просмотре» включает имена файлов, хранящихся на любом USB-накопителе, который вы подключаете к телевизору LG, скажем, с фотографиями, сделанными во время семейного отпуска. Исследователи провели еще один эксперимент, создав фиктивный видеофайл и загрузив его на USB-накопитель, который затем подключили к своему телевизору. Проанализировав сетевой трафик, они обнаружили, что имя этого видеофайла было передано в незашифрованном виде по протоколу HTTP и отправлено на адрес **GB.smartshare.lgtvsdp.com**.

Компания Sensory, которая разрабатывает встроенные решения для распознавания речи для умных устройств, считает, что может сделать в этом направлении еще больше. «Мы считаем, что магия [умных телевизоров] заключается в том, чтобы все время оставаться в режиме ожидания, — говорит Тодд Мозер, главный исполнительный директор компании Sensory. — Сейчас на [слушание] тратится слишком много энергии. Компания Samsung сделала действительно разумную вещь, разработав режим ожидания. Мы хотим пойти еще дальше и сделать так, чтобы телевизор все время оставался включенным и слушал независимо от того, где вы находитесь».

Теперь, когда вы знаете, на что способен ваш цифровой телевизор, вы, вероятно, спрашиваете себя: может ли ваш сотовый телефон подслушивать, находясь в выключенном состоянии? На этот вопрос существует три ответа: «да», «нет» и «сложно сказать».

В сообществе экспертов по вопросам защиты информации есть люди, которые утверждают, что необходимо вытащить аккумулятор из выключенного смартфона, чтобы быть уверенным в том, что он вас не подслушивает. Это не доказано и, похоже, является просто шуткой. Итак, есть люди, уверяющие нас в том, что достаточно просто выключить телефон и все. Однако я думаю, что на самом деле бывают случаи, например, если на смартфоне установлено вредоносное ПО, когда он не полностью отключается и по-прежнему может записывать разговоры, ведущиеся поблизости. Так что это зависит от множества факторов.

Существуют телефоны, которые «просыпаются», когда вы произносите волшебную фразу, подобно телевизорам с голосовым управлением. Это означает, что телефоны все время слушают, ожидая волшебной фразы. Это также подразумевает, что сказанное каким-то образом записывается или передается. Если на телефоне установлено вредоносное ПО, его камера или микрофон могут активироваться, когда пользователь по нему не разговаривает. Но, на мой взгляд, эти случаи весьма редки.

Однако вернемся к главному вопросу. В сообществе экспертов по вопросам конфиденциальности информации есть люди, настаивающие на возможности активировать телефон, когда он выключен. Существует вредоносное ПО, создающее впечатление того, что телефон выключен, когда на самом деле это не так. Однако возможность того, что кто-то может активировать выключенный телефон (при отсутствии питания от аккумулятора) представляется мне невероятной. В принципе, злоумышленник может использовать любое устройство с аккумулятором, позволяющим программному обеспечению находиться в рабочем состоянии. С помощью бэкдора в коде прошивки легко создать впечатление, что устройство выключено, когда это не так. В отсутствие питания устройство ничего не может сделать. Или может? Некоторые люди до сих пор утверждают, что АНБ установила в наши телефоны чипы, которые снабжают их электроэнергией и позволяют следить за нами, даже когда телефон физически выключен (то есть когда из него извлечен аккумулятор).

Таким образом, ваш смартфон, компьютер или автономное устройство на кофейном столике подключены к облачным сервисам, позволяющим устройствам реагировать на голосовые команды вроде: «Siri, где находится ближайшая заправочная станция?» Это означает, что они слушают.

И если это вас не беспокоит, знайте, что результаты поиска, осуществляемого этими сервисами, записываются и хранятся вечно.

Вечно.

Вне зависимости от того, способен ли ваш телефон вас подслушивать, браузер, который вы на нем используете, на это определенно способен. Примерно в 2013 году компания Google запустила расширение Google Voice Search Hotword с функцией голосового поиска, позволяющее с помощью простой голосовой команды активировать в браузере Chrome режим прослушивания. За ней последовали другие — компания Apple разработала систему Siri, корпорация Microsoft — систему Cortana, а компания Amazon — сервис Alexa. Таким образом, ваш смартфон, компьютер или автономное устройство на кофейном столике подключены к облачным сервисам, позволяющим устройствам реагировать на голосовые команды вроде: «Siri, где находится ближайшая заправочная станция?» Это означает, что они слушают. И если это вас не беспокоит, знайте, что результаты поиска, осуществляемого этими сервисами, записываются и хранятся вечно.

Вечно.

Итак, что же слышат эти устройства? На самом деле не ясно, что они делают, когда не отвечают на вопросы и не управляют телевизором. Например, проверив традиционную версию браузера Chrome для компьютера, исследователи обнаружили, что кто-то — Google? — по-видимому, все время подслушивает, используя микрофон компьютера. Эта функция попала в браузер Chrome из его версии с открытым исходным кодом под названием Chromium. В результате дальнейшего расследования они выяснили, что браузер включает микрофон по умолчанию. Несмотря на то что эта функция являлась частью программного обеспечения с открытым исходным кодом, она не была доступна для исследования.

С этим связано несколько проблем. Во-первых, программное обеспечение с открытым исходным кодом позволяет людям исследовать этот код, однако в данном случае фрагмент кода представлял собой черный ящик, поскольку его никто не проверял. Во-вторых, данный код попал в популярную версию браузера в процессе автоматического обновления, производимого компанией Google, от которого пользователи не могут отказаться. По состоянию на 2015 год компания Google так и не удалила его. Она предоставила людям возможность отказаться от использования этой функции, что, однако, требует наличия у них продвинутых навыков кодирования, поэтому среднестатистический пользователь не может сделать это самостоятельно.

Существуют и другие, более простые способы защиты от этой функции слежения в браузере Chrome и других программах. Что касается веб-камеры, просто заклейте ее непрозрачным скотчем. Одной из лучших защит для микрофона является установка заглушки, микрофонного штекера, в соответствующее гнездо на корпусе компьютера. Для этого возьмите старые сломанные наушники и просто отрежьте провод, оставив один штекер. Теперь вставьте этот штекер в гнездо для микрофона. Ваш компьютер будет ошибочно считать, что к нему подключен микрофон. Конечно, если вы захотите позвонить через Skype или какой-либо другой онлайн-сервис, вам сначала нужно будет вытащить этот штекер. Кроме того — и это очень важно, — убедитесь в том, что два провода микрофонного штекера не соприкасаются друг с другом, чтобы не повредить порт микрофона.

Помимо других устройств в доме работает умный динамик Amazon Echo, позволяющий пользователям голосовыми командами заказывать фильмы и другие товары в магазине Amazon. Echo также всегда находится во включенном состоянии в режиме ожидания, слушая каждое слово, ожидая «команды для пробуждения». Поскольку функционал Amazon Echo шире, чем у умного телевизора, перед тем как воспользоваться сервисом впервые, нужно наговорить ему примерно 25 разнообразных фраз, чтобы обучить его. Система Amazon может рассказать вам о погоде на улице, сообщить результаты последних спортивных соревнований, а также заказать тот или иной товар из ассортимента магазина, если вы попросите об этом. Учитывая общий характер некоторых фраз, распознаваемых системой Amazon, например: «Будет ли завтра дождь?», разумно предположить, что система Echo может слышать гораздо больше, чем ваш умный телевизор.

К счастью, компания Amazon предусмотрела способы удаления ваших голосовых данных из системы Echo. Если вы хотите удалить все данные (например, планируете продать кому-то свой динамик Echo), вам придется сделать это через сайт компании.

Несмотря на то что для пробуждения всех этих устройств, управляемых голосом, требуется ключевая фраза, все еще не ясно, что каждое из устройств делает, находясь в режиме ожидания, когда никто не дает ему никаких команд. По возможности отключайте функцию активации голосом в настройках устройства. При необходимости вы всегда сможете снова ее включить.

Теперь помимо системы Amazon Echo, телевизора и термостата к Интернету вещей присоединился и холодильник.

Холодильник?

Компания Samsung объявила о выпуске модели холодильника, которая подключается к вашему календарю Google для отображения предстоящих событий на плоском экране дверцы устройства, на месте которого раньше была простая белая поверхность. Только теперь холодильник подключается к Интернету через вашу учетную запись Google.

При разработке этого умного холодильника компания Samsung сделала несколько вещей. Она использовала соединение SSL/HTTPS для шифрования трафика между холодильником и сервером службы Google Календарь. Затем компания предоставила свой футуристический холодильник для тестирования в ходе DEF CON23 — одной из крупнейших хакерских конференций в мире.

Однако, согласно исследователям по вопросам безопасности Кену Мунро и Дэвиду Лоджу, которым ранее удалось взломать цифровой телевизор, компания Samsung не проверила сертификат, используемый при взаимодействии с серверами Google и при получении информации Google Календаря. Сертификат подтвердил бы безопасность соединения между холодильником и серверами Google. Однако без него злоумышленник мог бы создать свой собственный сертификат и перехватить трафик между холодильником и Google.

Ну и что?

Дело в том, что, подключившись к вашей домашней сети, злоумышленник может получить доступ не только к вашему холодильнику и заставить молоко и яйца испортиться, но и к вашей учетной записи Google, осуществив атаку посредника на программу-клиента холодильника, украсть ваши учетные данные для входа в систему Google, прочитать вашу электронную переписку, а может быть, нанести и гораздо более серьезный ущерб.

Умные холодильники пока еще не используются повсеместно. Однако разумно предположить, что по мере подключения все большего количества устройств к Интернету и даже к домашней сети мы будем сталкиваться с проблемами безопасности. И это вызывает опасения, особенно когда уязвимым может оказаться что-то очень личное и ценное, например ваш дом.

Компании, работающие в области Интернета вещей, разрабатывают приложения, способные превратить любое устройство в домашнюю систему безопасности. Например, телевизор может быть оснащен камерой. В этом случае с помощью установленных на смартфоне или планшете приложений вы сможете удаленно наблюдать за комнатой в вашем доме или офисе. А при обнаружении движения внутри дома или снаружи также может включаться освещение.

Рассмотрим сценарий: вы подъезжаете к своему дому, приложение системы охранной сигнализации на вашем смартфоне или в автомобиле узнает о вашем прибытии благодаря встроенной функции геолокации. На расстоянии пятнадцати метров от дома приложение передает домашней системе сигнализации команду разблокировать дверь дома или гаража (приложение на вашем смартфоне уже подключилось к дому и прошло процедуру аутентификации). Затем система сигнализации передает системе домашнего освещения команду включить свет на крыльце при входе в дом и, по желанию, в гостиной или на кухне. Кроме того, вам может захотеться, войдя в свой дом, услышать тихую классическую музыку или одну из последних популярных композиций из подборки музыкального сервиса вроде Spotify, воспроизводимую «умным» музыкальным центром. И конечно, при вашем возвращении температура в доме должна подниматься или понижаться, в зависимости от времени года и ваших предпочтений.

Домашние системы охранной сигнализации стали популярны в начале двадцать первого века. Тогда установка подобной системы предполагала монтаж проводных датчиков на дверях и окнах дома. Эти датчики подключались к единому концентратору, подключенному к обычной телефонной линии для отправки и получения сообщений от службы мониторинга. Вы активировали систему сигнализации, и если кто-либо пытался открыть двери или окна вашего дома, служба мониторинга связывалась с вами, как правило, по телефону. На случай аварийного отключения электропитания обычно был предусмотрен аккумулятор. Обратите внимание на то, что линия стационарного телефона могла перестать работать только в случае обрыва.

Когда многие люди избавились от привязки к стационарным телефонам и стали полагаться исключительно на сотовую связь, компании, занимающиеся мониторингом сигналов тревоги, начали предлагать свои услуги, основанные уже на ней. В последнее время они переключились на веб-сервисы.

Теперь на дверях и окнах устанавливаются беспроводные датчики. Однако, избавившись от необходимости протягивать уродливый кабель, мы столкнулись с большими рисками. Эксперты в области безопасности неоднократно замечали, что эти датчики не шифруют свой трафик. Злоумышленнику достаточно всего лишь перехватить сообщения, которыми обмениваются устройства, чтобы воспользоваться их уязвимостью. Например, если мне удастся получить доступ к вашей локальной сети, я смогу перехватить сообщения, которыми сервера вашей охранной компании обмениваются с устройством в вашем доме (если они передаются по той же локальной сети и не зашифрованы), и, манипулируя этими сообщениями, я могу управлять вашим «умным» домом, передавая ему подложные команды.

В настоящее время компании позволяют пользователю самому следить за своим домом. При срабатывании какого-либо из датчиков на ваш сотовый телефон приходит текстовое сообщение или специальное приложение позволяет увидеть изображение, полученное с установленной внутри дома веб-камеры. В любом случае вы сами все контролируете и наблюдаете за своим домом самостоятельно. И это здорово до тех пор, пока в вашем доме не отключится Интернет.

Даже при работающем Интернете злоумышленники могут вмешаться в работу беспроводных систем сигнализации. Например, атакующий может подавать ложные сигналы тревоги (за каждый из которых домовладельцу, скорее всего, придется платить). Устройства, вызывающие ложное срабатывание сигнализации, могут находиться перед вашим домом или на расстоянии до 230 метров. Слишком большое количество ложных сигналов тревоги может подорвать доверие к системе (и стоить домовладельцу огромных денег).

Кроме того, злоумышленник может создать помехи для сигнала беспроводного датчика с помощью радиошумов, чтобы нарушить его связь с концентратором или панелью управления. Это мешает

срабатыванию сигнала тревоги, фактически устраняя защиту и позволяя преступнику войти в дом.

Многие люди установили в своих домах веб-камеры — будь то для обеспечения безопасности, для наблюдения за уборщицей, няней, престарелым родственником, не выходящим из дома, или за любимым человеком, которому требуется особый уход. К сожалению, многие из этих работающих через Интернет веб-камер уязвимы для удаленных атак.

Существует общедоступная поисковая система под названием Shodan, позволяющая находить любые необычные устройства, подключенные к Интернету. Через Shodan можно обнаружить не только устройства из сферы Интернета вещей, работающие в домах, но и внутренние сети муниципальных коммунальных компаний и систем промышленного контроля, чьи сервера из-за неправильной конфигурации оказались доступны через публичный Интернет. Она также предоставляет доступ к бесчисленным видеопотокам с неправильно сконфигурированных коммерческих веб-камер, работающих по всему миру. Согласно оценкам, ежедневно около ста тысяч веб-камер передают данные через Интернет без какой-либо защиты.

Среди них есть веб-камеры компании D-Link, по умолчанию не предусматривающие прохождение процедуры аутентификации, которые могут использоваться для наблюдения за людьми и их личной жизнью (в зависимости от того, на что именно настроены эти камеры). Злоумышленник может использовать фильтры Google для поиска веб-камер D-link. Затем он может найти модели, по умолчанию не предусматривающие аутентификации, а затем перейти на веб-сайт вроде Shodan, щелкнуть по ссылке и на досуге просматривать транслируемое с них видео.

Чтобы этого не допустить, отключайте свои веб-камеры от Интернета, когда вы их не используете. Для большей уверенности отключайте их физически. При их использовании убедитесь, что на них настроена процедура аутентификации, а также установите сложный пароль вместо заданного по умолчанию.

Если вы считаете, что ваша персональная информация не защищена в вашем доме, подождите, пока не узнаете о том, что творится у вас на рабочем месте. Об этом мы поговорим в следующей главе.

Глава 13

СТУК БЕЗ ОТРЫВА ОТ ПРОИЗВОДСТВА

Если вы дочитали до этой страницы, значит вас явно беспокоит вопрос неприкосновенности частной жизни, однако у большинства из нас нет цели скрыть что бы то ни было от федерального правительства. Мы знаем, что наши работодатели могут видеть, чем мы занимаемся в Интернете во время работы (совершаем покупки, играем в игры, бездельничаем). Многим из нас хотелось бы защититься от подобного.

И это становится все труднее, причем отчасти благодаря сотовым телефонам, которые мы носим с собой. Всякий раз, когда Джейн Роджерс, финансовый менеджер Чикагской ландшафтной компании, хочет узнать, находятся ли ее сотрудники там, где они должны быть, она проверяет их реальное местонахождение на своем ноутбуке. Как и многие другие менеджеры и владельцы компаний, она использует для наблюдения за персоналом систему отслеживания объектов по GPS, установленную на служебных сотовых телефонах и автомобилях. Однажды клиент спросил у Джейн, выполнил ли один из ее сотрудников требуемые работы. Нажав пару клавиш, Джейн выяснила, что с 10:00 до 10:30 один из ее сотрудников находился в указанном месте.

Помимо геолокации, телематическая служба, используемая Роджерс, предоставляет и другие услуги. Например, она может просматривать любые фотографии, текстовые сообщения или электронные письма, отправленные сотрудниками с девяти принадлежащих ее компании смартфонов. Кроме того, у нее есть доступ к журналам вызовов и списку посещенных веб-сайтов. Однако Роджерс говорит, что использует только функцию GPS-отслеживания.

Мы знаем, что наши работодатели могут видеть, чем мы занимаемся в Интернете во время работы (совершаем покупки, играем в игры, бездельничаем). Многим из нас хотелось бы защититься от подобного.

Услуга GPS-отслеживания предоставляется уже давно. GPS и разработанный компанией United Parcel Service (UPS) алгоритм выбора маршрута под названием Orion позволили этой компании, занимающейся доставкой посылок, сократить расходы на горючее путем мониторинга и нахождения оптимальных маршрутов для своих водителей. Кроме того, она сумела найти управу на лентяев. Таким образом, компания UPS увеличила количество доставляемых за день посылок на 1,4 миллиона, сократив штат водителей на тысячу.

Все это хорошо для работодателей, которые утверждают, что, получив более высокую прибыль, они смогут больше платить своим сотрудникам. Но как себя чувствуют сотрудники? Для них наблюдение оборачивается определенными проблемами. В исследовании, проведенном журналом Harper’s, принимал участие водитель, за работой которого велось наблюдение с помощью электронных средств. Этот водитель, пожелавший остаться неизвестным, заявил о том, что программное обеспечение планировало его работу с точностью до секунды и оповещало его всякий раз, когда он опережал или отставал от оптимального графика. По словам водителя, к концу обычного рабочего дня он мог отставать от плана на целых четыре часа.

Где он прохлаждался? Водитель указал на то, что одна остановка могла предполагать доставку нескольких посылок, что не всегда учитывала программа ORION. Водитель рассказал о своих сотрудниках из нью-йоркского распределительного центра, которые страдали от хронических болей в спине и коленях из-за того, что пытались отнести слишком много посылок за один раз, стараясь не отставать от графика, составленного программным обеспечением, несмотря на постоянные напоминания компании о правилах обращения с тяжелыми грузами. Таким образом, с наблюдением за сотрудниками связаны определенные «человеческие издержки».

Другой сферой, в которой за персоналом регулярно следят, является индустрия общественного питания. Работа официантов отслеживается и оценивается программным обеспечением с помощью камер, встроенных в потолки ресторана и кассы операторов. В ходе исследования, проведенного в 2013 году специалистами из Университета Джорджа Вашингтона, Университета Бригама Янга и Массачусетского технологического института, было обнаружено, что программное обеспечение для обнаружения случаев воровства, используемое в 392 ресторанах, позволило снизить финансовый ущерб на 22 % с момента его установки. Как я говорил ранее, наблюдение за людьми меняет их поведение.

В настоящее время в Соединенных Штатах нет федеральных законов, запрещающих компаниям следить за работой своих сотрудников. Только в штатах Делавэр и Коннектикут работодатели обязаны ставить сотрудников об этом в известность. В большинстве штатов сотрудники понятия не имеют о том, наблюдает кто-то за их работой или нет.

Как насчет офисных сотрудников? Американская ассоциация менеджмента обнаружила, что 66 % работодателей контролируют использование Интернета своими сотрудниками, 45 % следят за

нажатиями клавиш на компьютере (воспринимая их отсутствие в качестве возможного «перерыва в работе»), а 43 % проверяют содержание электронной почты сотрудников. Некоторые компании контролируют записи в календаре Outlook своих сотрудников, заголовки электронных писем, а также журналы программ для обмена мгновенными сообщениями. Эти данные, по-видимому, используются компаниями для выяснения того, как их сотрудники тратят свое время: сколько времени продавцы тратят на работу с клиентами, с какими отделами компании осуществляется связь по электронной почте, сколько времени сотрудники тратят на совещания и сколько времени они проводят вне своих рабочих мест.

Конечно, есть и положительные последствия: наличие этих показателей позволяет компаниям более эффективно планировать встречи или побуждать сотрудников к более тесному взаимодействию. Однако суть состоит в том, что кто-то собирает все эти корпоративные данные. И когда-нибудь они могут быть переданы правоохранительным органам или, по крайней мере, использованы против вас при оценке эффективности вашей работы.

На работе вы не являетесь невидимкой. Все, что проходит через корпоративную сеть, принадлежит компании, а не вам. Даже если вы проверяете свою личную электронную почту, последний заказ в интернет-магазине или планируете отпуск, вы, вероятно, используете принадлежащий вашей компании смартфон, ноутбук или VPN-канал, поэтому будьте готовы к тому, что кто-то узнает обо всем, что вы делаете.

На работе вы не являетесь невидимкой. Все, что проходит через корпоративную сеть, принадлежит компании, а не вам. Даже если вы проверяете свою личную электронную почту, последний заказ в интернет-магазине или планируете отпуск, вы, вероятно, используете принадлежащий вашей компании смартфон, ноутбук или VPN-канал, поэтому будьте готовы к тому, что кто-то узнает обо всем, что вы делаете.

Вот простой способ защититься от слежки со стороны своего начальника и даже сотрудников: когда вы покидаете свое рабочее место, чтобы пойти на встречу или в туалет, заблокируйте компьютер. Я серьезно. Не оставляйте открытыми свой ящик электронной почты или данные, касающиеся проекта, на разработку которого вы потратили несколько недель, чтобы никто не смог его испортить. Заблокируйте экран компьютера на то время, пока будете отсутствовать. Это потребует лишь нескольких дополнительных секунд, но сэкономит вам много нервов. Установите в операционной системе таймер для блокировки экрана через определенное количество секунд бездействия. Или используйте специальное приложение с поддержкой интерфейса Bluetooth, которое автоматически блокирует компьютер, как только обнаруживает, что ваш смартфон не находится рядом с ним. Тем не менее для осуществления некоторых новых видов атак могут использоваться USB-устройства. Многие фирмы блокируют USB-порты своих ноутбуков и настольных компьютеров, но если в вашем офисе это не практикуется, то с помощью USB-накопителя злоумышленник сможет разблокировать ваш компьютер без ввода пароля.

Помимо корпоративных секретов в течение рабочего дня через наши компьютеры проходит множество личных писем, которые мы иногда распечатываем прямо в офисе. Если вас беспокоит конфиденциальность, не занимайтесь на работе никакими личными делами. Четко разделяйте свою профессиональную и личную жизнь. Или принесите из дома собственное устройство, например ноутбук или iPad, если намереваетесь решать частные вопросы во время перерыва. И если ваше мобильное устройство поддерживает функцию передачи данных через сотовую связь, никогда не используйте корпоративную сеть Wi-Fi и отключите широковещательную передачу идентификатора SSID, если вы настроили мобильную точку доступа (мобильный хотспот). При ведении личных дел на работе подключайтесь к Интернету только через оператора сотовой связи.

В самом деле, в офисе вы должны «носить маску», предназначенную для публики. Точно так же, как вы не говорите о личных делах со своими случайными сотрудниками, вам не следует заниматься личными делами, используя корпоративные компьютерные системы и сети (особенно в сферах, связанных со здоровьем или поиском новой работы).

Это сложнее, чем кажется. Во-первых, мы привыкли к вездесущности информации и почти повсеместной доступности Интернета. Однако если вы собираетесь овладеть искусством невидимости, вам придется отказаться от решения частных вопросов на публике.

Считайте, что все, введенное вами в офисный компьютер, общедоступно. Это не означает, что IT-отдел активно контролирует ваше конкретное устройство или когда-нибудь предпримет какие-либо действия по поводу того факта, что вы распечатали школьный проект своего ребенка на дорогостоящем цветном принтере, хотя они могут это сделать. Дело в существовании записи о ваших действиях, и если в будущем у начальства возникнут подозрения, оно сможет получить доступ к записям обо всем, что вы делали на конкретном компьютере. Этот компьютер принадлежит компании, а не вам. Как и сеть. Это означает, что компания сканирует все входящие и исходящие информационные потоки.

Рассмотрим случай Адама, который загрузил свой бесплатный кредитный отчет на рабочий

компьютер. Он авторизовался на сайте кредитного бюро с корпоративного компьютера, подключенного к корпоративной сети. Допустим, вы подобно Адаму просматриваете свой кредитный отчет на работе. Вы хотите распечатать его, не так ли? Так почему бы не сделать это с помощью стоящего в углу корпоративного принтера? Потому что в этом случае копия PDF-файла с вашей кредитной историей будет сохранена на жестком диске принтера. Вы не контролируете ни этот принтер, ни то, что произойдет с жестким диском после его списания. В настоящее время диски некоторых принтеров шифруются, но как вы можете быть уверены в том, что принтер в вашем офисе защищен? Никак.

Это еще не все. Каждый документ Word или Excel, созданный в Microsoft Office, содержит метаданные, описывающие этот документ. Обычно метаданные документа включают имя автора, дату создания, количество правок и размер файла, а также позволяют добавлять дополнительные сведения. Они не отображаются по умолчанию, и, чтобы их увидеть, вам нужно выполнить несколько дополнительных действий. Корпорация Microsoft предоставила инструмент «Инспектор документов», позволяющий удалить эти данные перед экспортом документа.

В результате исследования, проведенного в 2012 году при финансовой поддержке компаний Xerox и McAfee, было установлено, что 54 % сотрудников не всегда следуют корпоративной политике информационной безопасности, а 51 % сотрудников, на рабочем месте которых есть принтер, копир или многофункциональный принтер, заявили, что они копировали, сканировали или распечатывали на работе личную конфиденциальную информацию. И речь не только о рабочем месте, то же самое касается принтеров в местном копировальном центре или библиотеке. Все эти устройства оснащены жесткими дисками, которые запоминают все, что было напечатано за время их эксплуатации. Если вам нужно распечатать что-то личное, лучше сделать это позже, используя сеть и принтер, которые контролируете вы.

Процесс наблюдения за сотрудниками стал очень изощренным. Теперь для этого применяются офисные устройства, которые мы раньше воспринимали как само собой разумеющуюся и безопасную деталь обстановки, не предполагая, что и они могут использоваться для слежки.

Процесс наблюдения за сотрудниками стал очень изощренным. Теперь для этого применяются офисные устройства, которые мы раньше воспринимали как само собой разумеющуюся и безопасную деталь обстановки, не предполагая, что и они могут использоваться для слежки. Рассмотрим историю студента Колумбийского университета по имени Анг Цуй. Чтобы проверить, сможет ли он проникнуть во внутреннюю сеть компании и украсть конфиденциальные данные с помощью нетрадиционных средств, Цуй решил сначала атаковать лазерные принтеры, которые сегодня используются в большинстве офисов.

Цуй обнаружил, что принтеры безнадежно устарели. В процессе проведения нескольких тестов на проникновение я тоже это выяснил. Мне удалось использовать принтер для получения доступа к корпоративной сети. Это связано с тем, что сотрудники редко меняют пароль администратора на внутренних принтерах.

Программное обеспечение и прошивка принтеров, особенно коммерческих принтеров для домашнего офиса, имеют множество уязвимостей. Дело в том, что очень немногие воспринимают офисный принтер в качестве вектора атаки. Поэтому в этом случае работает принцип «безопасности через неясность» — если никто не замечает уязвимость, значит все в порядке.

Но как я уже говорил, у принтеров и копировальных машин, в зависимости от их модели, есть кое-что общее — они оснащены жесткими дисками. И если эти жесткие диски не зашифрованы, а это верно для очень многих из них, то к тому, что было напечатано, можно позднее получить доступ. Об этом известно уже давно. Цуй хотел проверить, можно ли использовать фирменный принтер против его владельцев и вынести то, что было напечатано, за пределы компании.

Чтобы было еще интереснее, Цуй решил атаковать код прошивки принтера, то есть программу, встроенную в микросхему, используемую внутри аппарата. В отличие от традиционных компьютеров и мобильных устройств, цифровые телевизоры и другие «умные электронные устройства» не обладают достаточной мощностью и ресурсами для поддержания работы полноценной операционной системы вроде Android, Windows или iOS. Вместо этого данные устройства используют так называемые операционные системы реального времени или ОСРВ (Real Time Operating Systems, RTOS), которые хранятся на отдельных чипах внутри устройства (часто это и называется прошивкой). На этих чипах хранятся только команды, необходимые для работы системы, и почти ничего сверх того. Иногда даже эти простые команды должны обновляться производителем или поставщиком путем перезаписи или замены чипа. Учитывая то, насколько редко это делается, становится очевидным, что многие производители просто не принимают надлежащих мер по обеспечению безопасности. Именно обновления Цуй решил использовать в качестве вектора атаки.

Цуй хотел выяснить, что произойдет, если взломать формат файла, используемый компанией Hewlett Packard для обновления прошивки, и обнаружил, что принтер Hewlett Packard не проверяет

аутентичность обновлений. Поэтому он создал собственную прошивку, и принтер ее принял. Только и всего. Принтер не проверял, что обновления действительно исходят от Hewlett Packard. Ему было достаточно лишь того, чтобы код был предоставлен в поддерживаемом формате.

Теперь Цуй мог работать свободно.

В ходе одного известного эксперимента Цуй обнаружил, что он может включить фьюзерный модуль (он же печка) принтера, который нагревает бумагу после нанесения на нее красителя, и оставить его работающим, что могло привести к возгоранию принтера. Продавец оборудования, но не компания Hewlett Packard, сразу ответил на это, заявив, что фьюзерный блок оснащен защитой от перегрева, так что принтер не мог загореться. Тем не менее Цуй показал, что эту защитную функцию можно отключить, поэтому принтер загореться все-таки мог.

После проведения этих экспериментов Цуй и его советник Сальваторе Столфо назвали принтеры слабым звеном в любом доме или организации. Представим ситуацию, что отдел кадров компании, входящей в Fortune 500, получил через Интернет вредоносный файл с резюме. За время, нужное менеджеру по кадрам, чтобы распечатать его, вся сеть, по которой пройдет документ, будет скомпрометирована, а вредоносное ПО установлено на подключенных к ней устройствах.

Для решения этой проблемы используется стратегия безопасной печати по требованию (pull printing), при которой документы отправляются на печать только после прохождения процедуры аутентификации (обычно в этом случае перед печатью документа пользователю необходимо ввести пароль). Для этого может использоваться PIN-код, смарт-карта или такие биометрические данные, как отпечаток пальца. Безопасная печать также предотвращает появление невостребованных документов, благодаря чему конфиденциальная информация не может оказаться на виду у всех.

Основываясь на результатах атак на принтеры, Цуй начал рассматривать другие потенциально уязвимые устройства, часто используемые в офисах, и в итоге остановил свой выбор на VoIP-телефоне (Voice over Internet Protocol).

Как и в случае с принтерами, никто не оценил их скрытую, но, если подумать, очевидную ценность для сбора информации. Как и в случае с принтером, поддельное обновление системы может быть принято VoIP-телефоном.

Большинство VoIP-телефонов предусматривают функцию Hands-free, которая позволяет вам включить в своем кабинете громкую связь. Это означает, что динамик и микрофон есть не только в телефонной трубке. Кроме того, телефон оснащен специальным переключателем, который сообщает ему о том, что трубка была снята с рычага или положена на рычаг, а также о включении громкой связи. Цуй понял, что, воспользовавшись уязвимостью этого рычага, он может прослушивать ведущиеся поблизости разговоры через микрофон для громкой связи даже при лежащей на рычаге телефонной трубке!

Один нюанс: в отличие от принтера, на который вредоносный код может попасть через Интернет, каждый телефон VoIP «обновляется» вручную. Для этого требуется, чтобы код распространялся с помощью USB-накопителя. Цуй решил, что это не проблема. За определенную плату нужные операции мог проделать ночной уборщик.

Цуй представил результаты своего исследования на нескольких конференциях, каждый раз используя разные VoIP-телефоны. В каждом случае производитель был заранее уведомлен об уязвимости, и каждый раз он ее исправлял. Однако Цуй отметил, что наличие патча не означает его применения. Во многих офисах, отелях и больницах могут до сих пор использоваться телефоны с неустраненной уязвимостью.

Итак, как же Цуй сумел получить данные с помощью телефона? Поскольку офисные компьютерные сети находятся под контролем, ему нужно было извлечь данные другим способом. Он решил пренебречь компьютерными сетями и использовать радиоволны.

Ранее исследователи из Стэнфордского университета и Израиля обнаружили, что нахождение вашего сотового телефона рядом с беспроводной клавиатурой позволяет третьему лицу подслушивать ваши разговоры. Для этого на ваше мобильное устройство необходимо установить вредоносное программное обеспечение. Однако, учитывая, что вредоносные программы можно загрузить из контролируемых мошенниками магазинов приложений, это достаточно просто, не так ли?

После установки на ваш смартфон вредоносного программного обеспечения акселерометр устройства становится достаточно чувствительным для того, чтобы уловить небольшие вибрации. По словам исследователей, в данном случае вредоносное программное обеспечение также может улавливать малейшие колебания воздуха, включая те, которые вызываются человеческой речью. Операционная система Android компании Google позволяет считывать показания с датчиков движения с частотой 200 Гц или 200 циклов в секунду. В большинстве случаев частотный диапазон

человеческого голоса составляет от 80 до 250 Гц. Это означает, что датчик может уловить значительную часть разговоров. Исследователи даже создали специальную программу распознавания речи, предназначенную для дальнейшей обработки сигналов в частотном диапазоне от 80 до 250 Гц.

Цуй обнаружил похожую уязвимость в VoIP-телефонах и принтерах. Он заметил, что ножки, которые есть почти у любой встроенной в современное устройство микросхемы, могут колебаться уникальным образом, а значит, передавать данные с помощью радиосигналов. Эта антенна, называемая «фантенна» (англ. Funtenna), предоставляет потенциальным злоумышленникам множество возможностей. Согласно официальному определению, сформулированному исследователем в сфере информационной безопасности Майклом Оссманном, которому Цуй приписывает авторство этой идеи, «фантенна — это используемая злоумышленником антенна, которая не разрабатывалась в качестве таковой при создании системы».

Что помимо «фантенн» можно использовать для слежки за сотрудниками?

Исследователи из Израиля обнаружили, что обычные сотовые телефоны с установленным на них вредоносным программным обеспечением могут получать от компьютеров двоичные данные. А чуть ранее исследователи из Стэнфорда выяснили, что датчики сотовых телефонов могут улавливать звук или электромагнитное излучение от беспроводной клавиатуры. Это исследование основано на аналогичных исследованиях, проведенных учеными из Массачусетского технологического института и Технологического института Джорджии. Достаточно сказать, что обо всем, что вы вводите, просматриваете или используете в офисе, может так или иначе узнать третья сторона.

Допустим, вы используете беспроводную клавиатуру. Радиосигнал, отправленный с клавиатуры на ноутбук или настольный ПК, может быть перехвачен. Сэми Камкар, исследователь по вопросам информационной безопасности, разработал фальшивое зарядное

USB-устройство под названием Keysweeper, которое перехватывает, расшифровывает, регистрирует и посылает обратно (через сеть GSM) данные обо всех нажатиях клавиш любой беспроводной клавиатуры Microsoft, находящейся поблизости.

Мы уже обсуждали опасность использования подложных точек доступа в кафе и аэропортах, маскирующихся под официальные. То же самое можно сказать и об офисах. Один из работников вашего офиса может настроить беспроводную точку доступа, к которой автоматически подключится ваше устройство. Сотрудники IT-отдела не всегда производят сканирование на предмет наличия таких устройств.

Сегодня для создания в офисе своей точки доступа достаточно принести собственное средство сотовой связи. Фемтосоты — это небольшие устройства, предоставляемые оператором сотовой связи. Они предназначены для улучшения качества сотовой связи внутри дома или офиса, то есть в местах со слабым сигналом. Эти устройства подвержены рискам утечки конфиденциальной информации.

Во-первых, поскольку фемтосоты представляют собой базовые станции сотовой связи, ваше мобильное устройство будет часто подключаться к ним, не сообщая об этом вам. Подумайте об этом.

В Соединенных Штатах правоохранительные органы используют устройство Stingray, также известное как IMSI-ловушка, ложная базовая станция. Кроме того, существуют устройства Triggerfish, Wolfpack, Gossamer и Swamp box. Несмотря на различия в технологии, в основном все эти устройства работают как фемтосоты без сотовой связи. Они предназначены для перехвата международного идентификатора мобильного абонента (International Mobile Subscriber Identity, IMSI) вашего сотового телефона. Пока в Европе эти устройства применяются гораздо шире, чем в Соединенных Штатах. Например, IMSI-перехватчики используются в ходе массовых акций протеста для того, чтобы правоохранительные органы могли идентифицировать их участников. Предполагается, что организаторы координируют мероприятие, находясь на связи.

В Соединенных Штатах правоохранительные органы используют устройство Stingray, также известное как IMSI-ловушка, ложная базовая станция. Кроме того, существуют устройства Triggerfish, Wolfpack, Gossamer и Swamp box.

После длительной юридической тяжбы Американский союз защиты гражданских свобод Северной Калифорнии (American Civil Liberties Union, ACLU) получил от правительства документы с подробным отчетом об использовании устройств Stingray. Например, правоохранительные органы получают судебный ордер на использование регистратора телефонных переговоров или отслеживающего устройства. Регистраторы применяются для перехвата набранных на телефоне номеров. Отслеживающее устройство используется для сбора информации о входящих вызовах. Кроме того, правоохранительные органы могут получить ордер на изъятие записи телефонного разговора или текста электронного сообщения. Согласно журналу *Wired*, в документах, полученных

ACLU, указывается, что устройства «могут перехватывать сообщения и, следовательно, данная функция в этих устройствах должна быть отключена и активироваться только при наличии ордера Title III», разрешающего перехватывать сообщение в режиме реального времени.

Допустим, правоохранительные органы за вами не следят. Предположим, вы находитесь в офисе, который строго контролируется, например, в офисе коммунальной службы. Кто-то может установить личную фемтосоту для обеспечения связи в обход обычной системы регистрации вызовов, используемой этой компанией. В данном случае опасность состоит в том, что сотрудник, установивший на своем столе модифицированную фемтосоту, может осуществить атаку посредника, а также подслушивать ваши телефонные разговоры или перехватывать текстовые сообщения.

Во время демонстрации на конференции Black Hat USA 2013 исследователям удалось перехватить разговоры, текстовые SMS-сообщения и даже веб-трафик находящихся в аудитории добровольцев с помощью фемтосот Verizon. Уязвимость фемтосот, выпущенных компанией Verizon, уже была исправлена, однако исследователи хотели показать, что их использования все равно следует избегать.

Некоторые версии Android оповещают вас при смене сотовой сети; смартфоны iPhone этого не делают. «Ваш телефон будет подключаться к фемтосоте без вашего ведома, — объяснил исследователь Дуг ДеПерри. — Это не похоже на Wi-Fi, в данном случае у вас нет выбора».

Компания Pwnie Express производит устройство под названием Pwn Pulse, позволяющее выявить фемтосоты и даже такие IMSI-перехватчики, как Stingray. Оно позволяет компаниям отслеживать работающие поблизости сотовые сети. Подобные инструменты для обнаружения полного спектра потенциальных угроз, относящихся к сотовой связи, раньше были доступны только государственным органам, но теперь это уже не так.

Несмотря на дружественность программы Skype к пользователю, она не является такой уж порядочной, когда речь идет о конфиденциальности данных. Согласно Эдварду Сноудену, чьи материалы впервые были опубликованы в газете Guardian, корпорация Microsoft сотрудничала с Агентством национальной безопасности (АНБ) в целях перехвата и контроля разговоров в Skype. В одном из документов говорилось о том, что программа АНБ под названием Prism отслеживает видеотрафик в Skype (среди прочих услуг связи). «Звук и ранее обрабатывался корректно, но без сопровождавшего его видеоизображения. Теперь аналитикам будет доступна полная “картина”», — пишет Guardian.

В марте 2013 года аспирант в области информатики из Университета Нью-Мексико обнаружил, что программа TOM-Skype, китайский вариант Skype, появившийся в результате сотрудничества корпорации Microsoft и китайской компании TOM Group, загружает списки ключевых слов на компьютер каждого пользователя Skype, поскольку в Китае существуют слова и фразы, которые не разрешается использовать в Интернете, например, «площадь Тяньаньмэнь». Кроме того, программа TOM-Skype отправляет правительству Китая имя пользователя, время и дату передачи, а также информацию о том, было ли сообщение отправлено или получено пользователем.

Исследователи обнаружили, что даже очень высокотехнологичные системы видеоконференций (не Skype, а платные программы) могут быть подвержены атакам посредника. Это означает, что сигнал направляется через кого-то другого, прежде чем достигнет вас. То же самое можно сказать и об аудиоконференциях. Если модератор не имеет списка номеров подключившихся и не прояснил непонятные номера, например, коды городов, находящихся за пределами Соединенных Штатов, то нет никакого способа убедиться в том, что к конференции не присоединился посторонний. В данной ситуации модератор должен связаться со всеми вновь подключившимися и в случае, если они не смогут идентифицировать себя, прервать соединение, и использовать резервный номер для конференц-связи.

Допустим, ваша фирма потратила большие деньги на покупку настоящей дорогостоящей системы конференц-связи. Вы можете подумать, что она более безопасна по сравнению с системой потребительского класса. Но вы ошибаетесь.

Рассмотрев эти высококлассные системы, исследователь Х. Д. Мур обнаружил, что почти все они по умолчанию автоматически «снимают трубку» в ответ на входящие видеовызовы. В этом есть смысл. Например, вы назначили конференцию на 10:00 утра и хотите, чтобы участники набрали номер в это время. Однако это также означает, что в другое время суток любой, у кого есть этот номер, также может набрать его и буквально подглядеть, что происходит в вашем офисе.

«Популярность систем для организации видеоконференций в сфере венчурного капитала и в финансовой отрасли означает существование ограниченного числа особо важных целей для того, кто намерен заниматься промышленным шпионажем или обеспечить себе в бизнесе несправедливое преимущество», — пишет Мур.

Насколько трудно обнаружить эти системы? Системы конференц-связи используют уникальный

протокол H.323. В небольшом сегменте Интернета Муру удалось выявить 250 000 систем, использующих данный протокол. Исходя из этого числа, он предположил, что менее пяти тысяч таких систем настроены на автоматический ответ — небольшой процент от общего количества, но довольно большое количество само по себе. И это, если не учитывать остальную часть Интернета.

Какую информацию может получить злоумышленник в результате взлома такой системы? Системная камера находится под контролем пользователя, поэтому человек, осуществляющий удаленную атаку, может направлять ее вверх, вниз, влево или вправо. В большинстве случаев камера не оснащена индикатором рабочего состояния, поэтому, если вы не смотрите на камеру, вы можете и не знать, что кто-то ею управляет. Кроме того, камера может масштабировать изображение. Мур сказал, что его исследовательская группа сумела прочитать шестизначный пароль, написанный на стене в шести метрах от камеры. Они также смогли прочитать электронное письмо с экрана пользователя, находившегося в другом конце комнаты.

В следующий раз, когда вы будете в офисе, подумайте о том, что можно увидеть через камеру системы видеоконференцсвязи. На стене может висеть схема организационной структуры отдела. Возможно, в обзор камеры попадает экран вашего компьютера, личные фотографии ваших детей и супруга или супруги. Это то, что может увидеть злоумышленник и, возможно, использовать против вашей компании или даже против вас самого.

Некоторые производители таких систем знают об этой проблеме. Например, компания Polycom предоставляет многостраничное руководство по усилению безопасности, включающее инструкции по ограничению движения камеры. Тем не менее сотрудники IT-отдела, как правило, не следуют подобным рекомендациям, а иногда даже не усматривают в этом проблем для безопасности. Тысячи систем конференц-связи в Интернете используют настройки по умолчанию.

Исследователи также обнаружили, что корпоративные брандмауэры не умеют обрабатывать протокол H.323. Исследователи предлагают предоставить устройству общедоступный интернет-адрес и настроить для него правило в корпоративном брандмауэре.

Самый большой риск заключается в том, что многие консоли администратора для систем конференц-связи практически не оснащены встроенными средствами обеспечения безопасности. В одном из примеров Муру и его сотрудникам удалось получить доступ к системе юридической фирмы, в которой содержался адрес зала заседаний совета директоров известного инвестиционного банка. Исследователи купили на аукционе eBay подержанное устройство для проведения видеоконференций и обнаружили на его жестком диске старые данные, включая адресную книгу с десятками личных номеров, многие из которых были настроены автоматически отвечать на входящие вызовы из Интернета в целом. Как и в случае со старыми принтерами и копировальными машинами, оснащенными жестким диском, прежде чем их продавать или дарить, необходимо тщательно стереть с них данные.

Иногда нам приходится работать над проектом совместно с коллегой, который может находиться в другой части света. Файлами можно обмениваться по корпоративной электронной почте, однако иногда они настолько объемны, что системы электронной почты просто не позволяют переслать их в качестве вложений. Все чаще люди используют сервисы обмена файлами для пересылки объемных документов.

Уровень безопасности таких облачных систем бывает разным.

Четыре крупнейших игрока: Apple iCloud, Google Drive, Microsoft OneDrive (ранее SkyDrive) и Dropbox — предусматривают двухэтапный процесс аутентификации. Это означает, что на ваше мобильное устройство отправляется код доступа для подтверждения вашей личности. И несмотря на то что все эти системы шифруют данные во время их пересылки, вам следует самостоятельно зашифровать их перед отправкой, если вы не хотите, чтобы сама компания или государственные службы получили к ним доступ.

На этом сходства заканчиваются.

Двухфакторная аутентификация (2FA) важна, но ее можно обойти путем захвата неиспользуемых учетных записей. Например, недавно я проверял систему клиента, который с помощью общедоступных инструментов добавил двухфакторную аутентификацию Google на свой веб-сайт, подключенный к VPN-сервису. Я сумел обойти ее, завладев учетными данными для доступа к службе Active Directory, принадлежащими пользователю, который не подписался на использование VPN-сервиса. Поскольку я был первым, кто подключился к VPN-сервису, мне было предложено настроить 2FA с помощью Google Authenticator. Если сам сотрудник так никогда и не получит доступ к сервису, то злоумышленник сможет и дальше его использовать.

Для хранимых данных сервис Dropbox использует 256-битное AES-шифрование (которое довольно надежно). Тем не менее оно предполагает сохранение ключей, которые могут предоставить Dropbox или правоохранительным органам несанкционированный доступ к данным. Сервисы Google Drive и

iCloud используют для данных в состоянии покоя значительно более слабое 128-битное шифрование. В данном случае существует опасность того, что данные могут быть дешифрованы с помощью больших вычислительных мощностей. Сервис Microsoft OneDrive не утруждает себя шифрованием, что заставляет думать о том, что это сделано специально, вероятно, по настоянию некоторых правительств.

Сервис Google Drive представил новую функцию управления правами на доступ к данным (Information Rights Management, IRM). В дополнение к документам, электронным таблицам и презентациям, созданным в Google Docs, система Google Drive теперь принимает файлы с расширением PDF и других форматов. К полезным функциям относится возможность запретить рецензентам и зрителям загрузку, печать и копирование. Вы также можете запретить предоставление другим пользователям доступа к общему файлу. Разумеется, эти функции управления правами на доступ к данным доступны только владельцам файлов. Это означает, что тот, кто поделился с вами файлом, должен устанавливать ограничения на доступ к нему.

Корпорация Microsoft также разработала уникальную функцию шифрования каждого отдельного файла, которая делает именно то, о чем говорит ее название: она шифрует каждый отдельный файл с помощью собственного ключа. Взлом одного ключа затронет только конкретный файл, а не весь архив. Тем не менее эта функция не используется по умолчанию, поэтому пользователям придется привыкнуть к самостоятельному шифрованию каждого файла.

В целом эта рекомендация кажется разумной. Сотрудники и пользователи должны привыкнуть к шифрованию данных перед их отправкой в «облако». Таким образом вы сохраняете контроль над ключами. Если государственная служба обратится в Apple, Google, Dropbox или Microsoft, то эти компании не смогут ей помочь, поскольку необходимые ключи будут у вас.

Вы также можете выбрать выделяющийся среди остальных сервис под названием SpiderOak, который предоставляет все преимущества облачного хранения и синхронизации, а также обеспечивает 100 % конфиденциальность данных. Сервис SpiderOak защищает конфиденциальные данные пользователя с помощью двухфакторной аутентификации и 256-битного AES-шифрования, что позволяет сохранять файлы и пароли в неприкосновенности. Пользователи могут хранить и синхронизировать чувствительную информацию с полной конфиденциальностью, поскольку этот облачный сервис отличается абсолютно нулевым разглашением паролей и данных.

Однако большинство пользователей будут продолжать использовать другие сервисы на свой страх и риск. Людям нравится легкость, с которой данные можно извлечь из «облака», и правоохранительным органам тоже. Огромная проблема при использовании «облака» заключается в том, что ваши данные не подпадают под защиту четвертой поправки в отличие от данных, хранящихся в ящике вашего стола или даже на вашем настольном компьютере. Правоохранительные органы запрашивают данные у облачных сервисов с вызывающей беспокойство частотой. И они могут получить к ним доступ с относительной легкостью, поскольку все, что вы загружаете в «облако», будь то веб-сервис электронной почты, Google Drive или ShutterFly, хранится на сервере, принадлежащем провайдеру облачных услуг, а не вам. Единственная истинная защита заключается в понимании того, что к загруженным в «облако» данным может получить доступ посторонний, и в принятии соответствующих мер, то есть в шифровании данных перед их отправкой.

Глава 14

АНОНИМНОСТЬ — ЭТО ТЯЖКИЙ ТРУД

Несколько лет назад я возвращался в Соединенные Штаты из поездки в Боготу, Колумбия, и когда прибыл в Атланту, два агента Таможенно-пограничной службы США отвели меня в отдельный кабинет. Учитывая то, что мне приходилось находиться под арестом и отбывать наказание в тюрьме, я, вероятно, волновался меньше, чем среднестатистический человек, оказавшийся в такой ситуации. Тем не менее мне было не по себе. Я не сделал ничего плохого. И я пробыл в этом кабинете четыре часа — на пять часов меньше максимального периода времени, в течение которого меня могли задержать без взятия под арест.

Проблемы начались, когда таможенный агент проверил мой паспорт, а затем уставился на экран. «Кевин, — сказал он, широко улыбаясь. — Знаете, кое-кто хочет поговорить с вами. Но вы не волнуйтесь. Все будет в порядке».

Я ездил в Боготу, чтобы выступить с речью, которую спонсировала газета El Tiempo. Я также посетил девушку, с которой встречался в то время. Находясь в кабинете таможенной службы, я позвонил своей девушке, которая жила в Боготе. Она сказала, что полиция Колумбии связалась с ней и попросила разрешения вскрыть посылку, которую я подготовил для отправки в США. «Они нашли следы кокаина», — сказала она. Я знал, что это не так.

В посылке находился 2,5-дюймовый внутренний жесткий диск. Видимо, колумбийские или американские власти хотели проверить его зашифрованное содержимое. Кокаин был просто предлогом для вскрытия посылки. Назад свой жесткий диск я так и не получил.

Позднее я узнал о том, что полицейские разорвали коробку, разобрали электронное оборудование и уничтожили жесткий диск моего ноутбука, когда пытались открыть его, просверлив в нем отверстие в поисках кокаина. Для вскрытия диска они могли бы использовать специальную отвертку. Наркотики они не нашли.

Тем временем в Атланте сотрудники таможенной службы открыли мой багаж и обнаружили мой MacBook Pro, ноутбук Dell XPS M1210, ноутбук Asus 900, три или четыре жестких диска, несколько USB-накопителей и Bluetooth-адаптеров, три смартфона iPhone и четыре сотовых телефона Nokia (каждый со своей SIM-картой, чтобы экономить средства на услугах сотовой связи в разных странах). Это стандартное оборудование для представителя моей профессии.

Кроме того, в моем багаже был комплект отмычек и устройство для клонирования, которое способно считывать и воспроизводить любую карту доступа HID proximity. Последнее может использоваться для извлечения учетных данных, хранящихся на картах физического доступа, путем его размещения в непосредственной близости от них. Например, я могу подделать учетные данные чьей-нибудь карты и открыть запертые двери, не создавая поддельную карту. Все это оказалось в моем багаже, поскольку в Боготе я проводил демонстрацию, касающуюся вопросов обеспечения безопасности. Естественно, когда сотрудники таможенной службы это увидели, их глаза загорелись, поскольку они решили, что я замышляю что-то вроде кражи данных банковских карт, что невозможно сделать с помощью этих устройств.

В конце концов, прибыли сотрудники Иммиграционной и таможенной полиции (Immigration and Customs Enforcement, ICE) и спросили, зачем я приехал в Атланту. Я собирался принять участие в экспертной дискуссии на конференции по безопасности, организованной Американским обществом промышленной безопасности (American Society for Industrial Security, ASIS). Позднее агент ФБР, участвующий в той же конференции, смог подтвердить причину моей поездки.

Все стало еще хуже, когда я открыл свой ноутбук и вошел в систему, чтобы показать им письмо, подтверждающее мое участие в конференции.

Мой браузер был настроен на автоматическую очистку истории при запуске, поэтому, когда я его запустил, открылось диалоговое окно, предлагающее мне очистить историю. Когда я подтвердил это действие, щелкнув по кнопке OK, агенты испугались. Но затем я просто нажал кнопку питания, чтобы выключить MacBook, так что теперь доступ к моему диску можно было получить только при наличии кодовой фразы PGP.

Поскольку я не был арестован, в чем меня неоднократно уверяли, я не был обязан называть свой пароль.

Даже если бы я был под арестом, законы США не обязывают меня выдавать свой пароль, однако соблюдение этого права зависит от того, как долго человек готов сопротивляться. Кроме того, в разных странах разные законы. Например, в Великобритании и Канаде власти могут заставить вас назвать свой пароль.

Спустя четыре часа сотрудники ICE и таможенной службы меня отпустили. Однако если бы мной заинтересовалось такое агентство, как АНБ, им, скорее всего, удалось бы добраться до содержимого моего жесткого диска. Государственные органы могут скомпрометировать прошивку вашего компьютера или смартфона, взломать сеть, используемую для подключения к Интернету, и использовать в своих целях различные уязвимости, обнаруженные в ваших устройствах.

Я могу путешествовать по зарубежным странам с еще более строгими законами и не сталкиваться с теми проблемами, которые возникают у меня в Соединенных Штатах из-за моей судимости. Итак, как выехать за границу с конфиденциальными данными? И как попасть во «враждебные» страны вроде Китая?

Если вы не хотите, чтобы на вашем жестком диске находились какие-либо конфиденциальные данные, сделайте следующее:

1. Удалите все конфиденциальные данные перед поездкой и выполните полное резервное копирование.

2. Оставьте конфиденциальные данные на диске, но зашифруйте их с помощью сильного ключа (хотя служащие некоторых стран могут заставить вас выдать ключ или пароль). Не храните ключ при себе.

Можно, например, хранить половину ключа за пределами Соединенных Штатов у друга, которого не смогут заставить выдать информацию.

3. Загрузите зашифрованные данные на облачный сервис, а затем скачивайте их по мере необходимости.

4. Используйте бесплатную программу шифрования, например VeraCrypt, для создания скрытой зашифрованной папки на вашем жестком диске. Опять же, если иностранное правительство найдет эту скрытую папку с файлами, оно может заставить вас выдать пароль.

5. Всякий раз при вводе пароля на своих устройствах накрывайте себя и свой компьютер, например, курткой или другим предметом одежды, чтобы ваши данные (и действия) не были зафиксированы камерой видеонаблюдения.

6. Запечатайте свой ноутбук и другие устройства в конверт FedEx или другой пакет из материала Тайвек, подпишите его и поместите в сейф в номере отеля. Если конверт будет поврежден, вы это заметите. Рассмотрите возможность покупки камеры, которую можно поместить в сейф, чтобы сделать снимок любого, кто его открыл, и в режиме реального времени отправить фотографию с помощью функции передачи данных через сотовую связь.

7. Но лучше всего не рисковать. Всегда носите устройства с собой и не выпускайте их из виду.

Согласно документам, полученным Американским союзом защиты гражданских свобод благодаря Закону о свободе информации, в период с октября 2008-го по июнь 2010-го более чем у 6500 человек, пересекших границу Соединенных Штатов, были проверены электронные устройства. Это значит, что за месяц на границе в среднем проверяется 300 электронных устройств. Почти половину всех путешественников составляли граждане США.

Малоизвестный факт: электронные устройства любого человека могут обыскать без ордера или разумного подозрения в пределах 160 км от границы США, то есть, вероятно, даже в Сан-Диего. Простой факт пересечения границы еще не означает, что вы в безопасности!

Малоизвестный факт: электронные устройства любого человека могут обыскать без ордера или разумного подозрения в пределах 160 км от границы США, то есть, вероятно, даже в Сан-Диего. Простой факт пересечения границы еще не означает, что вы в безопасности!

Основную ответственность за проверку пассажиров и предметов, въезжающих в Соединенные Штаты, несут два государственных учреждения: Управление таможенной и пограничной охраны при Министерстве национальной безопасности (CBP, Department of Homeland Security’s Customs and Border Protection) и Иммиграционная и таможенная полиция (ICE). В 2008 году Министерство национальной безопасности США объявило, что оно может проверить любое электронное устройство, попадающее на территорию Соединенных Штатов. Кроме того, оно представило так называемую Автоматизированную систему слежения (Automated Targeting System, ATS), которая мгновенно создает персональное и очень подробное досье, когда вы пересекаете границу. Управление таможенной и пограничной охраны использует ваше досье для принятия решения о том, будете ли вы подвергнуты более тщательному, а иногда и инвазивному обыску при повторном въезде в Соединенные Штаты.

Правительство США может забрать электронное устройство, проверить все файлы и подержать его еще некоторое время в целях дальнейшего изучения без каких-либо подозрений в ваш адрес.

Сотрудники пограничной охраны могут обыскивать ваше устройство, копировать его содержимое или попытаться восстановить удаленные изображения или видеофайлы.

Итак, вот что я делаю.

Для защиты своих данных и данных моих клиентов я шифрую конфиденциальные данные на своих ноутбуках. Находясь в чужой стране, я через Интернет передаю зашифрованные файлы для хранения на защищенных серверах, находящихся в любой точке мира. Затем я физически безвозвратно удаляю их с компьютера перед возвращением домой на случай, если правительственные чиновники решат обыскать или изъять мое оборудование.

Безвозвратное удаление данных — это не обычное удаление. При удалении данных изменяется только главная загрузочная запись для файла (индекс, используемый для поиска частей файла на жестком диске); файл (или некоторые его фрагменты) остается на жестком диске до тех пор, пока новые данные не будут записаны поверх соответствующей части жесткого диска. Именно это позволяет специалистам по цифровой криминалистике восстанавливать удаленные данные.

С другой стороны, безвозвратное удаление предполагает заполнение занимаемого файлом места случайными данными. На твердотельных дисках сделать это очень сложно, поэтому я ношу ноутбук с обычным жестким диском (HDD), на котором я выполняю эту процедуру, по крайней мере, 35 раз. При этом специальная программа сотни раз заполняет место удаляемого файла случайными данными, что значительно усложняет его восстановление.

Раньше я полностью копировал данные со своего устройства на внешний жесткий диск и зашифровывал их. Затем я отправлял резервный диск в Соединенные Штаты. Я не удалял данные у себя, пока мой коллега не подтверждал получение диска в рабочем состоянии. После этого я безвозвратно удалял личные файлы и файлы клиентов. Я не форматировал весь диск и не трогал операционную систему. Таким образом, в случае обыска мне было бы легче восстановить свои файлы удаленно, не переустанавливая всю операционную систему.

После происшествия в Атланте я несколько изменил свой подход. Я начал хранить у коллеги по бизнесу актуальные «клоны» своих компьютеров, используемых в поездках. Теперь мой коллега может просто отправить мне клонированные системы в любое место Соединенных Штатов.

Мой iPhone — другое дело. Если вы когда-нибудь подключите свой iPhone к ноутбуку для зарядки и нажмете кнопку подтверждения в диалоговом окне «Доверять этому компьютеру», то на компьютере будет храниться сертификат сопряжения, который позволяет компьютеру получить доступ ко всему содержимому iPhone без специального кода. Теперь сертификат сопряжения будет использоваться при подключении того же смартфона iPhone к этому компьютеру.

Например, если вы подключаете свой iPhone к компьютеру другого человека и доверяете ему, то между этим компьютером и устройством iOS будет установлена связь, позволяющая компьютеру получать доступ к фотографиям, видео, SMS-сообщениям, журналам вызовов, сообщениям WhatsApp и большинству других данных без введения кода доступа. Еще большее беспокойство вызывает то, что этот человек с помощью программы iTunes может сделать резервную копию всей памяти вашего смартфона, если только вы не установили пароль для создания зашифрованных резервных копий iTunes (что однозначно рекомендуется). Если вы не установили этот пароль, злоумышленник сам может его установить и без вашего ведома скопировать данные с мобильного устройства на свой компьютер.

Это означает, что, если правоохранительные органы захотят узнать, что хранится на вашем защищенном iPhone, они могут запросто подключить его к вашему ноутбуку, который, скорее всего, имеет действительный сертификат сопряжения со смартфоном. В данном случае лучше никогда не «доверять этому компьютеру», если только речь не идет о вашей персональной системе. Что, если вы хотите сделать недействительными все сертификаты сопряжения для вашего устройства Apple? Хорошая новость заключается в том, что вы можете сбросить сертификат сопряжения на своих устройствах Apple. Если вы хотите поделиться файлами с помощью устройства Apple, используйте технологию AirDrop. А при необходимости зарядить свой смартфон используйте кабель Lightning, подключая его к своему компьютеру или к адаптеру питания, а не к чужому компьютеру. Кроме того, на сайте synctop.com можно приобрести устройство USBCondom, блокирующее разъемы передачи данных в USB-порту, не трогая при этом разъемы питания. Например, подключив свой телефон через него, вы можете быть уверены, что его можно только зарядить, но не снять с него данные.

Что, если вы взяли с собой в путешествие только iPhone, но не взяли компьютер?

Я включил на своем iPhone функцию TouchID, чтобы смартфон распознавал отпечаток моего пальца. Перед прохождением иммиграционного контроля в любой стране я перезагружаю свой iPhone. И когда смартфон включается, я намеренно не ввожу свой код доступа. Несмотря на то что я включил функцию TouchID, она по умолчанию остается отключенной до ввода кода доступа. Судебные

инстанции США ясно понимают, что правоохранительные органы не могут потребовать от вас выдать свой пароль. По традиции в Соединенных Штатах вас не могут заставить давать свидетельские показания; однако вас могут вынудить повернуть ключ в замке сейфа. Таким образом, суд может заставить вас предоставить отпечатки пальцев для разблокировки устройства. Простым решением является перезагрузка смартфона. Таким образом, функция распознавания отпечатка не будет включена и вам не придется выдавать свой код доступа.

Тем не менее в Канаде это закон; если вы являетесь гражданином Канады, вы обязаны предоставить свой код доступа по первому требованию. Так и случилось с Аленом Филиппоном из Сент-Анн-де-Плейнс, Квебек. Возвращаясь домой из Пуэрто-Платы, провинции Доминиканской Республики, он отказался предоставить сотрудникам пограничной службы Новой Шотландии код доступа к своему смартфону. Ему было предъявлено обвинение в соответствии с разделом 153.1 (б) канадского Закона о таможне за то, что он препятствовал сотруднику таможенной службы в выполнении им своих обязанностей в рамках этого закона. В случае признания виновным человек обязан заплатить штраф в размере 1000 долларов США, при этом максимальным наказанием является штраф в 25 000 долларов и вероятность тюремного заключения сроком на один год.

Я знаю о канадском законе, касающемся паролей, не понаслышке. В 2015 году я воспользовался сервисом Uber, чтобы доехать из Чикаго в Торонто (погода была нелетной), и когда мы пересекли границу между штатом Мичиган и Канадой, нас отправили на дополнительную инспекцию. Возможно, это было связано с тем, что за рулем сидел парень с Ближнего Востока, у которого была только грин-карта. В пункте проведения дополнительной инспекции произошла сцена, достойная сериала «C.S.I.: Место преступления».

Агенты таможенной службы убедились в том, что мы покинули автомобиль, оставив внутри все свои вещи, включая наши сотовые телефоны. Нас с водителем развели в разные стороны. Один из агентов подошел к водительскому месту и взял его смартфон. Он потребовал у водителя код доступа и начал исследовать содержимое его устройства.

До этого я уже решил никогда не выдавать свой пароль. Я чувствовал, что мне придется выбирать между выдачей своего пароля и разрешением на въезд в Канаду. Поэтому я решил воспользоваться техникой социальной инженерии.

Я крикнул таможенному агенту, который обыскивал смартфон водителя: «Эй, вы же не собираетесь обыскивать мой чемодан, верно? Он заперт, поэтому вы не можете это сделать». Это сразу привлекло ее внимание. Она сказала, что имеет полное право обыскать мой чемодан.

Я ответил: «Я запер его, поэтому его нельзя обыскать».

В следующее мгновение два агента подошли ко мне и потребовали ключ. Я начал спрашивать, зачем им обыскивать мой чемодан, а они снова объяснили, что они имеют право обыскивать все что угодно. Я вытащил свой бумажник и передал агенту ключ от моего чемодана.

Этого было достаточно. Они совершенно забыли о сотовых телефонах и сосредоточились на моем чемодане. Миссию удалось выполнить путем перенаправления внимания. Меня отпустили и, к счастью, никогда уже не спрашивали пароль от моего смартфона.

В ситуации обыска легко потерять ориентацию. Не позволяйте себе стать жертвой обстоятельств. Проходя через любой контрольный пункт, убедитесь в том, что ваш ноутбук и электронные устройства лежат на конвейерной ленте последними. Вам не нужно, чтобы ваш ноутбук находился на другом конце, в то время как кто-то впереди вас задерживает очередь. Кроме того, если вам нужно выйти из очереди, не забудьте забрать свой ноутбук и электронное устройство.

Защита конфиденциальных данных, которой мы можем наслаждаться дома, не обязательно распространяется на путешественников, оказывающихся на границе США. В случае с врачами, юристами и многими бизнес-профессионалами инвазивный обыск на границе может поставить под угрозу конфиденциальность данных, связанных с их профессиональной деятельностью. Эти данные могут включать врачебную, коммерческую или адвокатскую тайну, исследовательские и бизнес-стратегии, некоторые из которых путешественник обязан сохранять в соответствии с законом или условиями договора.

Для остальных людей обыск жестких дисков и мобильных устройств может нарушить конфиденциальность электронной почты, данных о состоянии здоровья и даже финансовой информации. Имейте в виду, что недавние поездки в определенные страны, которые считаются недружественными по отношению к США, могут обусловить применение дополнительных мер контроля со стороны сотрудников пограничной службы.

Репрессивные правительства представляют собой еще одну проблему. Они могут настаивать на более тщательном обследовании ваших электронных устройств, чтении электронной почты и проверке папки «Загрузки». Также существует вероятность (особенно если они изымут у вас

ноутбук), что они попытаются установить на ваше устройство программное обеспечение для слежения.

Многие компании выдают выезжающим за границу сотрудникам одноразовые телефоны и ноутбуки для временного пользования. По возвращении сотрудника в Соединенные Штаты либо эти устройства выбрасываются, либо данные на них безвозвратно удаляются. Однако для большинства из нас загрузка зашифрованных файлов в «облако» или покупка нового устройства и избавление от него по возвращении не являются целесообразными.

В общем, без особой необходимости не берите с собой электронные устройства с конфиденциальной информацией. Если вы все-таки их берете, попробуйте обойтись минимальным их количеством. И если вам нужно взять с собой мобильный телефон, вероятно, имеет смысл использовать одноразовое устройство во время своего путешествия. Тем более что стоимость звонков и пересылки данных в роуминге чрезвычайно высока. Лучше взять разблокированный одноразовый телефон и приобрести SIM-карту в той стране, куда вы направляетесь.

Без особой необходимости не берите с собой электронные устройства с конфиденциальной информацией. Если вы все-таки их берете, попробуйте обойтись минимальным их количеством. И если вам нужно взять с собой мобильный телефон, вероятно, имеет смысл использовать одноразовое устройство во время своего путешествия. Тем более что стоимость звонков и пересылки данных в роуминге чрезвычайно высока.

Вы можете подумать, что прохождение таможенного контроля — это самая кошмарная часть любой поездки. Однако обыскать могут и ваш номер в отеле.

В 2008 году я совершил несколько поездок в Колумбию помимо той, после которой меня задержали в Атланте. Во время одной из поездок, совершенных мной в том году, в моем номере в Боготе произошло нечто странное. И это был не какой-нибудь сомнительный отель; это была одна из гостиниц, где часто останавливались колумбийские чиновники.

Возможно, в этом и была проблема.

Я отправился на ужин со своей девушкой, и когда мы вернулись, индикатор моего дверного замка загорелся желтым цветом, когда я вставил ключ. Не зеленым. Не красным. Желтый цвет индикатора обычно означает, что дверь заперта изнутри.

Я спустился к стойке регистрации и попросил у клерка новую ключ-карту. Индикатор снова загорелся желтым цветом. Я повторил все сначала. Тот же результат. После третьего раза я убедил служащих отеля отправить со мной кого-нибудь. Дверь открылась.

Внутри ничего не вызвало подозрений. Фактически тогда я просто убедил себя в том, что замок был неисправным. Только вернувшись в Соединенные Штаты, я понял, что произошло.

Прежде чем покинуть Соединенные Штаты, я позвонил своей бывшей девушке, Дарси Вуд, которая раньше работала техническим руководителем Tech TV, и попросил ее приехать ко мне домой и заменить жесткий диск на моем ноутбуке Macbook Pro. В то время жесткие диски Macbook Pro было нелегко извлечь. Однако ей это удалось. Вместо старого диска она установила новый, мне пришлось его отформатировать и установить операционную систему macOS.

Несколько недель спустя, когда я вернулся из этой поездки в Колумбию, я попросил Дарси снова приехать ко мне в Лас-Вегас, чтобы заменить диски.

Она сразу же заметила, что изменилось. Она сказала, что кто-то затянул винты жесткого диска намного сильнее, чем она. Очевидно, кто-то в Боготе вынул диск, вероятно, для копирования его содержимого, когда меня не было в номере.

Совсем недавно то же самое произошло со Стефаном Эссером, исследователем, хорошо известным благодаря взлому продуктов iOS. Он опубликовал в Twitter фотографию своего неправильно установленного на место жесткого диска.

Даже на диске с небольшим количеством данных содержится какая-то информация. К счастью, я использовал программу PGP Whole Disk Encryption компании Symantec для шифрования всего содержимого моего жесткого диска. (Вы также можете использовать программу WinMagic для операционной системы Windows или FileVault 2 в среде macOS.) Таким образом, копия содержимого моего жесткого диска абсолютно бесполезна в отсутствие ключа для его разблокировки. Именно из-за того, что, как мне кажется, произошло в Боготе, в путешествии я теперь всегда беру свой ноутбук с собой, даже отправляясь на ужин. Если я не могу этого сделать, я никогда не оставляю его в спящем режиме. Я его выключаю. Если ноутбук не выключен, то злоумышленник может создать файл дампа памяти и получить мои ключи шифрования PGP Whole Disk. Поэтому я отключаю свой ноутбук.

В начале книги мы говорили о множестве предосторожностей, которые использовал Эдвард Сноуден для обеспечения конфиденциальности информации, которой он обменивался с Лорой Пойтрас. Когда украденные Сноуденом секретные данные были готовы к обнародованию, ему и Пойтрас понадобилось выбрать место для их хранения. Такие распространенные операционные системы, как Windows, iOS, Android и даже Linux, не лишены уязвимостей. Это касается любого программного обеспечения. Поэтому им нужна была безопасная операционная система, зашифрованная с самого начала и не доступная без специального ключа.

Шифрование жесткого диска работает следующим образом: при загрузке компьютера вы вводите безопасный пароль, вернее, кодовую фразу типа «We don’t need no education» из знаменитой песни группы Pink Floyd. Затем загружается операционная система, и вы можете получить доступ к своим файлам и выполнять любые задачи, не замечая при этом никакой задержки, поскольку драйвер осуществляет прозрачное шифрование в режиме реального времени. Тем не менее, если вы оставите свое устройство без присмотра хотя бы на мгновение, существует вероятность того, что кто-нибудь сможет получить доступ к вашим файлам (поскольку они разблокированы). Запомните: когда ваш зашифрованный жесткий диск разблокирован, вам необходимо принять меры предосторожности, чтобы сохранить его в безопасности. Как только вы выключите компьютер, ключ шифрования престанет быть доступным для операционной системы, то есть он исчезнет из памяти, и к хранящимся на диске данным нельзя будет получить доступ..

Tails — это операционная система, которая может быть запущена на любом современном компьютере, чтобы не оставлять на его жестком диске (предпочтительно защищенном от записи) никаких данных, которые можно было бы восстановить. Установите Tails на DVD-диск или USB-накопитель, а затем настройте последовательность загрузки устройств в BIOS или EFI (macOS), выбрав DVD-диск или USB-накопитель для запуска Tails. Будет запущена операционная система, предусматривающая несколько инструментов для обеспечения конфиденциальности, в том числе Tor Browser. Эти инструменты позволяют шифровать электронную почту с помощью PGP, шифровать USB-накопители и жесткие диски, а также защищать сообщения с помощью протокола OTR (Off-the-Record Messaging).

Вместо всего жесткого диска вы можете зашифровать отдельные файлы. Бесплатный инструмент TrueCrypt по-прежнему доступен, но больше не поддерживается и не обеспечивает полного шифрования диска. Отсутствие поддержки не позволяет устранить любые актуальные уязвимости. Если вы продолжаете использовать программу TrueCrypt, учитывайте эти риски. Альтернативой TrueCrypt 7.1a является программа VeraCrypt, которая представляет собой продолжение проекта TrueCrypt.

Также существует несколько платных программ. Одной из них является Windows BitLocker, которая, как правило, включается в профессиональные версии операционной системы Windows. Для работы с BitLocker откройте программу Проводник Windows (Windows Explorer), щелкните правой кнопкой мыши по логическому диску C и в открывшемся контекстном меню выберите пункт **Включить BitLocker** (Turn on BitLocker). BitLocker задействует специальную микросхему на вашей материнской плате — доверенный платформенный модуль (Trusted Platform Module, TPM). Он разблокирует ключ шифрования только после подтверждения того, что ваша программа-загрузчик не была изменена. Это идеальная защита от атак типа Evil Maid («злая горничная»), о которых я расскажу чуть позже. Вы можете настроить BitLocker на разблокировку при включении устройства, или только при вводе ПИН-кода, или при наличии специального USB-устройства. Последние варианты намного безопаснее. У вас также есть возможность сохранить ключ в своей учетной записи Microsoft. Не делайте этого, поскольку в этом случае вы предоставите корпорации Microsoft свои ключи (которыми, как вы увидите далее, она может уже обладать).

У инструмента BitLocker есть несколько недостатков. Во-первых, он использует генератор псевдослучайных чисел (pseudorandom number generator, PRNG) под названием Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generator), который может содержать бэкдор, встроенный АНБ. Также этот инструмент является проприетарным, то есть вам придется поверить корпорации Microsoft на слово, что он работает и не содержит никаких бэкдоров АНБ, в отличие от программного обеспечения с открытым исходным кодом. Еще одним недостатком BitLocker является то, что вам придется предоставить корпорации Microsoft ключ, если вы не готовы приобрести его за 250 долларов. Если вы этого не сделаете, правоохранительные органы могут запросить ключ у корпорации Microsoft.

Несмотря на эти оговорки, Фонд электронных рубежей (англ. Electronic Frontier Foundation, EFF) фактически рекомендует BitLocker среднестатистическому потребителю, который хочет защитить свои файлы. Однако имейте в виду, что защиту BitLocker можно обойти.

Другим коммерческим инструментом является PGP Whole Disk Encryption компании Symantec. Его используют многие университеты и корпорации. Я тоже раньше его применял. Программа PGP Whole Disk Encryption была создана Филом Циммерманом, разработавшим технологию PGP для электронной почты. Как и BitLocker, PGP использует микросхему TPM для проведения процедуры дополнительной аутентификации при включении ПК. Бессрочная лицензия стоит около 200

долларов.

Также существует WinMagic, один из немногих инструментов, предусматривающих двухфакторную аутентификацию в дополнение к использованию пароля. Кроме того, WinMagic не применяет мастер-пароль. Вместо этого зашифрованные файлы группируются, и каждая группа имеет свой пароль. Это может затруднить восстановление пароля, поэтому данный вариант подходит не для всех.

Для компьютеров Apple предусмотрен инструмент FileVault2. После его установки вы можете активировать FileVault2, для чего запустите приложение **Системные настройки** (System Preferences), щелкните по значку **Безопасность и конфиденциальность** (Security & Privacy), а затем перейдите на вкладку **FileVault**. Опять же не следует хранить ключ шифрования в своей учетной записи Apple. Это предоставит компании доступ к вашим данным, который она, в свою очередь, может предоставить правоохранительным органам. Вместо этого выберите вариант **Создать ключ восстановления и не использовать мою учетную запись iCloud** (Create a recovery key and do not use my iCloud account), а затем распечатайте или запишите ключ, состоящий из 24 символов. Сохраните этот ключ в тайне, поскольку любой, кто его найдет, может разблокировать ваш жесткий диск.

Если вы используете iOS8 или более поздние версии этой операционной системы на iPhone или iPad, то содержимое этих устройств шифруется автоматически. Компания Apple сделала еще один шаг вперед, заявив, что ключ хранится в памяти устройства, то есть у пользователя. Это означает, что правительство США не может запросить у Apple ключ: он уникален для каждого устройства. Директор ФБР Джеймс Коми утверждает, что подобный подход к шифрованию — не такая хорошая вещь, как можно было бы подумать. В своем выступлении он сказал: «Изощренные преступники станут использовать эти способы для предотвращения своего обнаружения. И я спрашиваю: какова цена?» В данном случае речь идет о том, что информация о преступлениях будет недоступна для расшифровки.

В 1990-е годы тот же самый страх задержал рассмотрение моего судебного дела на несколько месяцев, в течение которых я томился в тюрьме. Мои юристы хотели получить доступ к сведениям, которые правительство планировало использовать против меня во время судебного разбирательства. Правительство заявило, что не передаст никакие зашифрованные файлы, если я не предоставлю ключ шифрования. Я отказался. В свою очередь суд отказался обязать правительство предоставить эти сведения, поскольку я не выдал им свой ключ.

Устройства под управлением операционной системы Android, начиная с версии 3.0 (Honeycomb), также могут быть зашифрованы. Большинство из нас предпочитает этого не делать. Начиная с Android 5.0 (Lollipop), шифрование дисков используется по умолчанию в смартфонах Nexus с ОС Android, но опционально в устройствах других производителей, например, LG, Samsung и др. Если вы решите зашифровать свой смартфон под управлением операционной системы Android, имейте в виду, что на это может уйти около часа, при этом ваше устройство должно быть подключено к источнику питания во время всего процесса. По имеющимся сообщениям, шифрование вашего мобильного устройства не оказывает существенного влияния на его производительность, однако после принятия решения о шифровании вы не сможете в дальнейшем передумать.

При использовании любой из этих программ для полного шифрования диска всегда остается вероятность существования бэкдора. Однажды меня наняла компания для тестирования USB-продукта, который позволял пользователям хранить файлы в зашифрованном контейнере. Во время анализа кода мы обнаружили, что разработчик внедрил в него секретный бэкдор — ключ для разблокировки зашифрованного контейнера хранился в случайном расположении на USB-накопителе. Это означает, что любой, кому известно местоположение ключа, может разблокировать зашифрованные пользователем данные.

Еще хуже то, что компании не всегда знают, что делать с этой информацией. Когда я завершил анализ безопасности зашифрованного USB-устройства, генеральный директор позвонил мне и спросил, следует ли ему оставить бэкдор на месте или нет. Он беспокоился о том, что правоохранительным органам или АНБ может потребоваться доступ к данным пользователя. Тот факт, что он решил об этом спросить, весьма красноречив.

В отчете о прослушивании телефонных разговоров за 2014 год правительство США сообщило о том, что оно столкнулось с зашифрованными дисками только в 25 устройствах из 3554, на которых осуществлялся поиск доказательств. При этом им удалось расшифровать диски на двадцати одном из двадцати пяти устройств. Таким образом, несмотря на то что шифрование часто позволяет защитить данные от обычного вора, для правительства, твердо решившего добиться своего, это не проблема.

Несколько лет назад исследователь Йоанна Рутковская написала о том, что она назвала атакой Evil Maid («злая горничная»). Допустим, кто-то оставляет в гостиничном номере выключенный ноутбук с жестким диском, зашифрованным с помощью программы TrueCrypt или PGP Whole Disk

Encryption. (В Боготе я использовал инструмент PGP Whole Disk Encryption и выключил свой ноутбук.) Позднее кто-то входит в номер и подключает к ноутбуку USB-накопитель с вредоносным загрузчиком. Затем ноутбук должен быть запущен с этого USB-накопителя для установки вредоносного загрузчика, который похищает кодовую фразу. Ловушка установлена.

Горничная, то есть кто-то, кто может часто посещать гостиничный номер, не вызывая подозрений, была бы лучшим кандидатом для осуществления этой атаки — отсюда и название. Горничная может зайти практически в любой гостиничный номер на следующий день и ввести секретную комбинацию для извлечения кодовой фразы, которая была тайно записана на диск. Теперь злоумышленник может ввести эту кодовую фразу и получить доступ ко всем вашим файлам.

Я не знаю, сделали ли то же самое с моим ноутбуком в Боготе. Сам жесткий диск был извлечен, а затем установлен на место, при этом винты оказались затянуты слишком сильно. В любом случае мой диск, к счастью, не содержал важной информации.

Как насчет помещения ваших электронных устройств в сейф отеля? Это лучше, чем оставлять эти ценные вещи на виду или в чемоданах? Да, но ненамного. На время участия в недавней конференции Black Hat я остановился в отеле Four Seasons в Лас-Вегасе. Я положил в сейф 4000 долларов наличными, несколько банковских карт и чеков. Через несколько дней я попытался открыть сейф, но код не подошел. Я вызвал сотрудников службы безопасности, и они открыли сейф. Я сразу заметил, что пачка стодолларовых банкнот значительно уменьшилась. В ней осталось 2000 долларов. Итак, куда делись другие 2000 долларов? Сотрудники службы безопасности отеля не имели ни малейшего понятия. Мой друг, занимающийся физическим тестированием на проникновение, попытался взломать сейф, но у него ничего не получилось. Эта история по-прежнему остается загадкой. По иронии судьбы, этот сейф назывался Safe Place (безопасное место).

Немецкая компания G-DATA, занимающаяся разработкой антивирусов, обнаружила, что в гостиничных номерах, в которых останавливались ее исследователи, для сейфа «чаще всего» использовался пароль по умолчанию (0000). В подобных случаях независимо от выбранного вами секретного пароля любой, кто знает пароль по умолчанию, также может получить доступ к вашим ценным вещам. Компания G-DATA подтвердила, что это выяснялось не систематически, а случайно на протяжении нескольких лет .

Немецкая компания G-DATA, занимающаяся разработкой антивирусов, обнаружила, что в гостиничных номерах, в которых останавливались ее исследователи, для сейфа «чаще всего» использовался пароль по умолчанию (0000).

Если злоумышленник не знает пароль по умолчанию для сейфа в данном конкретном гостиничном номере, он может открыть его методом грубой силы. Несмотря на то что у менеджера отеля есть аварийное электронное устройство для открытия сейфа, подключающееся к USB-порту, опытный вор может просто отвинтить пластину на передней панели сейфа и использовать цифровое устройство для открытия расположенного под ней замка. Кроме того, он может вызвать короткое замыкание и сбросить настройки, чтобы ввести новый пароль.

Если это вас не обеспокоило, подумайте вот о чем. Компания G-DATA также обнаружила, что данные с устройства для считывания банковских карт в сейфах номеров отеля, с помощью которых вы часто оплачиваете их использование, могут быть прочитаны посторонними, которые могут украсть данные банковской карты, а затем использовать или продать их через Интернет.

В настоящее время для запирания и отпирания двери номера в отелях используются NFC-карты или карты с магнитной полосой. Преимущество заключается в том, что сотрудники отеля могут быстро и легко изменять эти коды доступа со стойки регистрации. Если вы потеряете свою карту, то сможете запросить новую. В замок отправляется простой код, и к тому моменту, когда вы доберетесь до своего номера, новая ключ-карта будет работать. Инструмент MagSpoof, созданный Сэми Камкаром, можно использовать для подбора правильных последовательностей для замка двери гостиничного номера, открываемого с помощью карт с магнитной полосой. Этот инструмент использовался в одном из эпизодов сериала «Мистер Робот».

Использование магнитной полосы или NFC-чипа породило слух о том, что персональная информация может храниться на ключ-картах, используемых в отелях. Это не так. Однако городская легенда продолжает распространяться. Существует очень распространенная история о заместителе шерифа округа Сан-Диего, который якобы выпустил предупреждение о том, что на ключ-карте отеля были обнаружены имя постояльца, его домашний адрес и реквизиты банковской карты. Вероятно, вы получали электронное письмо примерно следующего содержания:

«Сотрудники правоохранительных органов Южной Калифорнии, которым было поручено выявление новых угроз для конфиденциальности персональных данных, недавно обнаружили, какая информация хранится на используемых в отелях ключ-картах.

Несмотря на то что в разных отелях используются разные ключи, ключ, полученный у сети отелей

Double Tree для использования на региональной презентации, посвященной проблеме кражи персональных данных, содержит следующую информацию:

• Имя клиента;

• Частично — домашний адрес клиента;

• Номер комнаты в отеле;

• Дата заезда и дата выезда;

• Номер банковской карты клиента и срок ее действия!

Когда вы сдаете эти ключ-карты на стойке регистрации, ваша личная информация становится доступной любому сотруднику, который может просто просмотреть ее с помощью специального сканера. Сотрудник может взять домой несколько карт и, используя сканирующее устройство, перенести информацию на ноутбук и совершить покупки за ваш счет.

Проще говоря, отели не стирают данные с этих карт до их выдачи следующему постояльцу. Обычно они хранится в ящике у стойки регистрации с ВАШЕЙ ИНФОРМАЦИЕЙ НА НИХ!!!

Суть в том, что вам следует брать карты себе или уничтожать их! НИКОГДА не оставляйте и НИКОГДА не сдавайте их на стойке регистрации при отъезде из отеля. Плату за них с вас не возьмут».

По поводу правдивости того, что написано в этом письме, было много споров. По-моему, это полная чушь.

Указанная информация, безусловно, может храниться на ключ-карте, однако это кажется слишком неправдоподобным даже мне. В отелях для каждого постояльца используется что-то вроде токена, числового идентификатора. Связать этот токен с конкретным постояльцем можно только при наличии доступа к серверу, используемому для выставления счетов.

Я не считаю, что вам нужно собирать и уничтожать старые ключи, однако вам, вероятно, все равно захочется это сделать.

Вот еще один распространенный вопрос, касающийся защиты ваших данных во время путешествия: что зашифровано в штрих-коде в нижней части вашего билета на самолет? Что он может о вас рассказать? По правде говоря, не так уж и много, если вы не участвуете в программе поощрения часто летающих пассажиров и не имеете идентификационного номера в ней.

Начиная с 2005 года Международная ассоциация воздушного транспорта (Air Transport Association, IATA) решила использовать посадочный талон со штрихкодом, поскольку применение посадочных талонов с магнитной лентой требовало слишком больших затрат. Согласно оценкам, это должно было позволить сэкономить 1,5 млрд долларов США. Кроме того, использование штрих-кодов на авиабилетах позволяет пассажирам загрузить свой билет из Интернета и распечатать его дома или использовать при посадке вместо него смартфон.

Излишне говорить, что эта измененная процедура потребовала введения некоего стандарта. По словам исследователя Шона Юинга, в штрих-коде на типичном посадочном талоне зашифрована довольно безвредная информация: имя пассажира, название авиакомпании, номер места, аэропорт отправления, аэропорт прибытия и номер рейса. Однако наиболее чувствительной частью штрих-кода является ваш номер часто летающего пассажира. В настоящее время все авиакомпании защищают учетные записи клиентов на своих веб-сайтах персональными паролями. Номер часто летающего пассажира — это, конечно, не номер социального страхования, но все равно его обнародование представляет собой нарушение конфиденциальности ваших данных.

Еще большая проблема связана с картами лояльности, предлагаемыми супермаркетами, аптеками, заправочными станциями и другими предприятиями. В отличие от авиабилетов, которые оформляются на ваше имя, при выдаче карты лояльности можно назвать вымышленное имя, адрес и номер телефона (вымышленный номер, который вы в состоянии запомнить), поэтому между вами и вашим потребительским поведением невозможно будет установить связь.

Когда вы приходите в свой отель и включаете компьютер, вы можете обнаружить в списке доступных сетей Wi-Fi сети с такими названиями, как «Постоялец отеля», «tmobile123», «iPhone Кимберли», «attwifi», «Android Стива» и «Точка доступа Чака». К какой из них вам следует подключиться? Надеюсь, вы уже знаете ответ!

В большинстве отелей в сети Wi-Fi шифрование не используется, а для прохождения процедуры аутентификации требуется фамилия постояльца и номер комнаты. Разумеется, существуют приемы, позволяющие обойти систему платного доступа.

Один из способов бесплатно пользоваться Интернетом в любом отеле заключается в том, чтобы позвонить в любой номер, например через коридор, и представиться сотрудником отеля. Если в отеле определяется номер вызывающего абонента, позвоните с телефона в фойе. Сообщите ответившему на звонок человеку о том, что заказанные им два бутерброда уже в пути. Когда постоялец скажет, что он ничего не заказывал, вежливо спросите его фамилию, чтобы исправить ошибку. Теперь у вас есть номер комнаты (вы в нее звонили) и фамилия, и это все, что требуется (не платящему за Интернет гостю) для прохождения процедуры аутентификации в качестве законного постояльца данного отеля.

Предположим, вы остановились в пятизвездочном отеле, предоставляющем платный или бесплатный доступ в Интернет. При входе в систему вы можете увидеть сообщение о доступном обновлении продукта компании Adobe (или какого-либо другого разработчика). Как приличному пользователю, вам может захотеться загрузить обновление и продолжить работу. Однако сеть отеля следует считать потенциально небезопасной, даже если для доступа к ней используется пароль. Это не ваша домашняя сеть, поэтому обновление может быть ненастоящим, и если вы загрузите его, то рискуете установить на свой ПК вредоносный код.

Если подобно мне вы много путешествуете, то обновление является для вас серьезной проблемой. Вы мало что можете сделать, кроме как удостовериться в том, что обновление действительно существует. Проблема в том, что при использовании Интернета в отеле для загрузки этого обновления вы можете быть перенаправлены на поддельный веб-сайт, содержащий вредоносное «обновление». По возможности используйте свое мобильное устройство, чтобы подтвердить наличие обновления на сайте производителя программного обеспечения, и если оно не является критически важным, подождите, пока не сможете воспользоваться для его загрузки безопасной сетью, например, в офисе компании или дома.

Хакеры выясняют имена руководителей компаний, которые должны остановиться в том или ином роскошном отеле, а затем ожидают их прибытия, разместив на сервере отеля вредоносное ПО. Когда руководитель вселяется и подключается к сети Wi-Fi отеля, вредоносная программа загружается и выполняется на его устройстве. После заражения вредоносная программа удаляется с сервера отеля. Как отмечают исследователи, это происходит на протяжении почти десятилетия.

Исследователи из Лаборатории Касперского, разрабатывающей системы защиты от киберугроз, выявили использующую эти методы группу преступников-хакеров, которую они назвали DarkHotel (другое ее название Tapaoux). Эти хакеры выясняют имена руководителей компаний, которые должны остановиться в том или ином роскошном отеле, а затем ожидают их прибытия, разместив на сервере отеля вредоносное ПО. Когда руководитель вселяется и подключается к сети Wi-Fi отеля, вредоносная программа загружается и выполняется на его устройстве. После заражения вредоносная программа удаляется с сервера отеля. Как отмечают исследователи, это происходит на протяжении почти десятилетия.

Несмотря на то что это в первую очередь касается руководителей, которые останавливаются в роскошных отелях Азии, такая тактика может использоваться и в других местах. Как правило, группа DarkHotel использует низкоуровневые целевые фишинговые атаки для массовых целей и оставляет атаки на серверы отелей для более важных целей, например, руководителей, работающих в сфере ядерной энергетики и обороны.

В результате проведения первичного анализа было высказано предположение о том, что группа DarkHotel базировалась в Южной Корее. В коде применяемого в ходе атак клавиатурного шпиона — вредоносного программного обеспечения для записи нажатий клавиш в уязвимых системах — были обнаружены корейские символы. А также уязвимости нулевого дня (уязвимости, о которых неизвестно компании-разработчику) представляли собой весьма существенные, не известные ранее изъяны в программном обеспечении. Кроме того, была обнаружена связь южнокорейского имени в коде клавиатурного шпиона с другими сложными клавиатурными шпионами, использовавшимися корейцами в прошлом.

Однако следует отметить, что этого недостаточно для подтверждения. Код программного обеспечения может браться из разных источников. Кроме того, программное обеспечение может выглядеть так, как если бы оно было создано в одной стране, когда фактически оно создано в другой.

Для установки вредоносного программного обеспечения на ноутбуки группа DarkHotel использует поддельные сертификаты, которые выглядят так, будто они выданы правительством Малайзии и компанией Deutsche Telekom. Как вы помните из главы 5, сертификаты используются для проверки происхождения программного обеспечения или веб-сервера. Чтобы еще больше запутать следы, хакеры сделали так, чтобы вредоносное программное обеспечение находилось в бездействии на протяжении шести месяцев, а затем активировалось. Это делалось для того, чтобы сотрудники IT-отделов не могли установить связь между поездкой и заражением.

Исследователи Лаборатории Касперского узнали об этой атаке только тогда, когда компьютеры

группы ее клиентов оказались зараженными после пребывания в конкретных роскошных отелях Азии. Исследователи обратились к стороннему сервису Wi-Fi, который использовался в обоих отелях, и совместно с ним решили проверить, что происходит в его сетях. Несмотря на то что файлы, используемые для заражения компьютеров постояльцев, давно исчезли, были обнаружены записи об удалении файлов, совпадающие с периодом их пребывания в отеле.

Самый простой способ защититься от подобных атак — подключиться к службе VPN сразу после подключения к Интернету в отеле. Я использую недорогой сервис, который обходится мне в шесть долларов в месяц. Однако это не очень хороший выбор, если вы хотите остаться невидимым, поскольку он не позволяет производить анонимную настройку.

Если вы хотите быть невидимым, не предоставляйте сервису VPN реальные данные о себе. Для этого вам потребуется заранее зарегистрировать поддельный адрес электронной почты и использовать открытую беспроводную сеть. После регистрации поддельного адреса электронной почты используйте сеть Tor, чтобы настроить биткойн-кошелек, найдите биткойн-банкомат для пополнения этого кошелька, а затем используйте биткойн-миксер для того, чтобы ваши операции невозможно было отследить через блокчейн. Для отмывания биткойнов необходимо открыть два биткойн-кошелька, используя разные цепочки узлов сети Tor. Первый кошелек используется для отправки биткойнов в биткойн-миксер, а второй — для получения уже отмытых биткойнов.

Обеспечив анонимность благодаря месту с бесплатным Wi-Fi вне зоны видимости камеры видеонаблюдения и сети Tor, найдите сервис VPN, который принимает биткойны в качестве оплаты. Оплатите услугу с помощью «отмытых» биткойнов. Некоторые сервисы VPN, включая Witopia, блокируют Tor Browser, поэтому вам нужно найти сервис, который его не блокирует, желательно, чтобы провайдер VPN-услуг не вел логов.

В данном случае мы не предоставляем сервису VPN свой реальный IP-адрес или имя. Тем не менее при использовании вновь настроенной службы VPN вы должны быть осторожны и не использовать какие-либо сервисы от своего реального имени и не подключаться к службе VPN с IP-адреса, который можно связать с вами. Вы можете рассмотреть возможность использования анонимно приобретенного одноразового телефона.

Лучше всего купить портативную точку доступа, причем приобрести ее нужно максимально анонимно. Например, вы можете нанять кого-нибудь для ее покупки, чтобы ваше лицо не попало в камеру, установленную в магазине. При использовании анонимной точки доступа вам следует отключить все персональные устройства, предусматривающие средства сотовой связи, чтобы предотвратить их регистрацию в местах работы точки доступа и таким образом не допустить формирования соответствующей ассоциации с вами.

Подведем итог. Вот что необходимо сделать для анонимного использования Интернета в путешествии:

1. Анонимно приобретите предоплаченные подарочные карты. В Европейском Союзе это можно сделать на сайте **viabuy.com**.

2. Используйте открытую сеть Wi-Fi после изменения своего MAC-адреса.

3. Найдите сервис электронной почты, допускающий регистрацию без подтверждения с помощью SMS-сообщения. Или зарегистрируйте телефонный номер Skype, используя сеть Tor и предоплаченную подарочную карту. Это позволит вам принимать голосовые вызовы для подтверждения вашей личности (но только не в кофейнях Starbucks или в других местах с установленными камерами видеонаблюдения). Используйте сеть Tor при регистрации электронной почты, чтобы скрыть свое местоположение.

4. Используя новую анонимную электронную почту, зарегистрируйтесь на сайте типа **paxful.com**, используя все тот же Tor Browser, чтобы открыть биткойн-кошелек и купить биткойны. Заплатите за них с помощью предоплаченных подарочных карт.

5. Зарегистрируйте второй анонимный адрес электронной почты и второй биткойн-кошелек после смены цепочки узлов Tor, чтобы их невозможно было связать с первым электронным ящиком и биткойн-кошельком.

6. Используйте сервис для отмывания биткойнов, например **bitlaunder.com**, чтобы затруднить отслеживание операций с ними. Отмытые биткойны будут отправлены на второй биткойн-кошелек.

7. Отмытыми биткойнами оплатите услугу VPN от провайдера, который не регистрирует трафик или IP-подключения. Обычно собираемые данные перечислены в политике конфиденциальности (например, VPN-сервис TorGuard).

8. Обзаведитесь одноразовой портативной точкой доступа, попросив кого-нибудь приобрести ее для вас. Для ее покупки дайте человеку наличные.

9. Для доступа в Интернет используйте точку доступа вдали от домашних, рабочих и других сотовых устройств.

10. После включения устройств подключитесь к сервису VPN через точку доступа.

11. Используйте Tor Browser для посещения сайтов.

Глава 15

СПЕЦСЛУЖБАМ ВСЕГДА УДАЕТСЯ ПОЙМАТЬ НУЖНОГО ЧЕЛОВЕКА

В отделе научной фантастики публичной библиотеки Сан-Франциско в Глен-Парке, недалеко от своей квартиры, Росс Уильям Ульбрихт вел переписку в чате с клиентом своей компании. В то время — в октябре 2013 года — человек, с которым он переписывался, полагал, что имеет дело с администратором сайта, пользовавшимся псевдонимом Dread Pirate Roberts («ужасный пират Робертс»), взятым из фильма «Принцесса-невеста». Робертс, также известный как DPR, был не кто иной, как Росс Ульбрихт — администратор и владелец онлайн-магазина наркотиков Silk Road, на которого охотились федеральные власти. Ульбрихт часто использовал для работы общественные точки доступа Wi-Fi, например в библиотеке, вероятно, ошибочно полагая, что агенты ФБР, если они когда-либо идентифицируют его как пользователя с ником DPR, никогда не произведут рейд в общественном месте. Однако в тот день человек, с которым общался Ульбрихт, оказался тайным агентом ФБР.

Управление онлайн-магазином наркотиков, в котором клиенты могли анонимно приобрести кокаин и героин, а также широкий спектр синтетических наркотических веществ, требовало определенных умений. Сайт был размещен в Даркнете, и доступ к нему можно было получить только через Tor Browser. В качестве валюты сайт принимал только биткойны. И создатель магазина Silk Road был осторожен, но недостаточно.

За несколько месяцев до того, как Ульбрихт оказался в окружаемой агентами ФБР публичной библиотеке Сан-Франциско, у одного человека появились доказательства, позволяющие связать Ульбрихта с ужасным пиратом Робертсом. Этим человеком был агент Налогового управления США по имени Гэри Элфорд, который следил за публикациями, посвященными магазину Silk Road и его возникновению, а по вечерам исследовал эту тему с помощью расширенного поиска в системе Google. Одно из самых ранних упоминаний о Silk Road появилось в 2011 году. Кто-то под ником «altoid» обсуждал его в одном из чатов. Поскольку в 2011 году сайт Silk Road еще не был запущен, Элфорд посчитал, что пользователь altoid, скорее всего, обладал инсайдерской информацией. Разумеется, Элфорд начал искать другие доказательства.

Как выяснилось, он наткнулся на золотую жилу.

Очевидно, пользователь altoid разместил свой вопрос и в другом чате, а исходное сообщение удалил. Элфорд обнаружил ответ на уже удаленный вопрос, содержащий исходное сообщение. В этом сообщении пользователь altoid написал, что тот, кто готов ответить на его вопрос, может связаться с ним по адресу rossulbricht@gmail.com.

Это был не последний раз, когда Ульбрихт допустил подобную оплошность. Он задавал вопросы и на других сайтах, например Stack Overflow: исходный вопрос был отправлен от имени , которое позднее удивительным образом поменялось на DPR.

Правило номер один искусства быть невидимым: никогда не связывайте свою анонимную онлайн-личность с реальной. Никогда не делайте этого.

В дальнейшем были установлены другие связи. Ульбрихт, как и DPR, исповедовал принципы свободного рынка и либертарианства, которые продвигал Рон Пол. И в какой-то момент Ульбрихт даже заказал набор поддельных водительских удостоверений с разными именами из разных штатов, что в июле 2013 года привело к порогу его квартиры в Сан-Франциско федеральных агентов, которые в то время и не подозревали, что имеют дело с человеком, пользующимся псевдонимом DPR.

Со временем данные стали достаточно убедительными для того, чтобы одним октябрьским утром 2013 года, когда начался вышеупомянутый разговор с клиентом, федеральные агенты вошли в библиотеку Глен-Парка. Там они молниеносно схватили Ульбрихта, прежде чем он смог закрыть свой ноутбук. Если бы он успел это сделать, некоторые ключевые доказательства были бы уничтожены. Как бы то ни было, федеральным агентам удалось сделать снимки экранов панели системного администрирования сайта под названием Silk Road сразу после ареста и тем самым установить конкретную связь между Ульбрихтом, пользователем под ником Dread Pirate Roberts и магазином Silk Road, уничтожив все его надежды на сохранение анонимности.

В то октябрьское утро в Глен-Парке Ульбрихт был зарегистрирован в системе Silk Road в качестве администратора. И агенты ФБР знали об этом, поскольку наблюдали за его компьютером в Интернете. Но что, если бы он мог подделать данные о своем местоположении? Что, если бы он находился не в библиотеке, а использовал бы вместо этого прокси-сервер?

Летом 2015 года исследователь Бен Каудилл из компании Rhino Security объявил о том, что на конференции DEF CON23 он не только собирается представить свое новое устройство ProxyHam, но и намерен прямо там продавать его по цене около 200 долларов. Затем, примерно неделю спустя,

Каудилл объявил, что его выступление было отменено, а все существующие устройства ProxyHam подлежат уничтожению. Больше никаких объяснений от него не последовало.

Выступления на крупных конференциях по безопасности могут быть отменены по разным причинам. Либо производители, которые должны быть на них представлены, либо федеральное правительство оказывают давление на исследователей, чтобы они не обнародовали свои данные. Однако в нашем случае Каудилл не собирался указывать на какой-то конкретный существующий изъян; он создал нечто новое.

У Всемирной паутины есть забавное свойство — появившаяся в ней идея, как правило, остается там навсегда. Поэтому если бы федеральные агенты или кто-то другой убедил Каудилла в том, что его выступление не отвечает интересам национальной безопасности, скорее всего, это новое устройство создал бы кто-то другой. Именно так и случилось.

ProxyHam представляет собой удаленную точку доступа. Ее использование подобно установке передатчика Wi-Fi в вашем доме или офисе. Только в данном случае использующий и контролирующий ProxyHam человек может находиться на расстоянии до полутора километров. Передатчик Wi-Fi использует радиочастоту 900 МГц для подключения к внешней антенне компьютера, находящегося на расстоянии до четырех километров. Таким образом, в случае с Россом Ульбрихтом агенты ФБР могли собираться возле библиотеки Глен-Парка, а он в это время мог находиться в чьем-нибудь подвале в нескольких кварталах от нее.

Потребность в таких устройствах очевидна, если вы живете в стране с тоталитарным режимом. Общение с внешним миром через сеть Tor — это риск, на который идут многие. Такое устройство добавило бы еще один уровень безопасности, позволив скрыть местоположение пользователя.

Правда кто-то не хотел, чтобы Каудилл говорил об этом на конференции DEF CON.

В интервью Каудилл отрицал, что Федеральная комиссия по связи (Federal Communications Commission, FCC) отговорила его от выступления. Журнал *Wired* предположил, что тайная установка ProxyHam в чужой сети может рассматриваться как несанкционированный доступ в соответствии с принятым в США драконовским и неоднозначным законом «О компьютерном мошенничестве и злоупотреблении». Каудилл не прокомментировал эти предположения.

Я уже говорил о том, что появившейся в Интернете идеей может воспользоваться любой человек. Исследователь в области информационной безопасности Сэми Камкар создал устройство ProxyGambit, по сути, заменившее ProxyHam. Оно отличается только использованием обратного сотового трафика, поэтому вы можете находиться не то что в нескольких километрах от устройства, а в другой части света. Круто!

Устройства, подобные ProxyGambit, разумеется, послужат причиной головной боли для правоохранительных органов, когда преступники решат ими воспользоваться.

Созданный Ульбрихтом сайт Silk Road представлял собой онлайн-магазин наркотиков. Это не то, что можно было найти через поисковую систему Google; эта площадка не находилась на «поверхности» Всемирной паутины, как те ресурсы, которые можно легко индексировать и находить. Поверхностная паутина (Surface Web) включает в себя такие всем известные сайты, как Amazon и YouTube, и на нее приходится всего 5 % всех ресурсов, размещенных в Интернете. Известные и посещаемые большинством из вас веб-сайты составляют мизерную часть от их фактического количества. Бóльшая часть веб-сайтов на самом деле скрыта от большинства поисковых систем.

После поверхностной паутины следующей крупнейшей частью Интернета является так называемая «Глубокая паутина» (Deep Web). Доступ к этой части Всемирной паутины осуществляется с помощью паролей. Например, содержимое каталога публичной библиотеки Сан-Франциско в Глен-Парке. Глубокая паутина также включает большую часть сайтов, доступ к которым предоставляется только по подписке, а также сайты корпоративных интрасетей. Netflix. Pandora. Ну, вы поняли.

Наконец, существует небольшая часть Всемирной паутины под названием «Даркнет» (Darknet, «Темная паутина»). К ней невозможно получить доступ через обычный браузер, а существующие в ней сайты нельзя найти через такие поисковые системы, как Google, Bing или Yahoo!.

Даркнет — это место, где наряду с магазином Silk Road существуют сайты, на которых вы можете нанять убийцу и приобрести детскую порнографию. Такие сайты работают в Даркнете, поскольку он позволяет сохранять почти полную анонимность. Я говорю «почти», поскольку не существует ничего абсолютного.

Доступ к Даркнету осуществляется только через Tor Browser. На самом деле веб-сайты Даркнета имеют сложные буквенно-цифровые URL-адреса, оканчивающиеся — .onion. Как я уже упоминал, луковый маршрутизатор (Onion Router) был разработан Военно-морской научно-исследовательской лабораторией США для того, чтобы дать людям в тоталитарных странах возможность связаться друг

с другом и с кем-то, находящимся за пределами их стран. Я также объяснил, что Tor не подключает ваш браузер напрямую к сайту; вместо этого он устанавливает связь с другим сервером, который в свою очередь соединяется с *еще одним* сервером, чтобы, в конце концов, добраться до места назначения. Многократное перенаправление затрудняет отслеживание. И такие сайты, как Silk Road, являются результатом работы скрытых сервисов сети Tor. Их URL-адреса генерируются с помощью алгоритма и часто меняются. С помощью Tor можно получить доступ как к Поверхностной, так и к Темной паутине (Даркнету). Еще одним средством, с помощью которого можно получить доступ к веб-сайтам Поверхностной и Темной паутины (Даркнета), является сеть I2P.

Еще до закрытия магазина Silk Road некоторые люди предполагали, что АНБ или кто-то другой может идентифицировать пользователей в Даркнете. Одним из способов является определение и анализ компьютеров, называемых выходными узлами, точками, в которых интернет-запрос в расшифрованном виде передается одному из скрытых сервисов, хотя это все равно не позволяет идентифицировать того, кто послал исходный запрос.

Для этого ведущее слежку правительство должно установить, что запрос был сделан на доступ к сайту X и что за несколько секунд до этого кто-то в Нью-Гэмпшире запустил Tor Browser. В данном случае наблюдающий может заподозрить наличие связи между этими двумя событиями. Со временем одномоментный доступ к этому сайту и подключение к сети Tor могут превратиться в закономерность. Во избежание этого следует сделать так, чтобы Tor Browser работал постоянно.

Ульбрихта погубила неаккуратность. У него, по-видимому, с самого начала не было никакого плана. В своих ранних сообщениях, касающихся магазина Silk Road, он поочередно использовал свой настоящий адрес электронной почты и псевдоним.

Как видите, в современном мире очень сложно использовать Интернет, не оставляя следов своей подлинной личности. Но, как я говорил в начале книги, существуют способы, с помощью которых вы тоже можете овладеть искусством быть невидимым. На следующих страницах я покажу вам, как это сделать.

Ульбрихта погубила неаккуратность. У него, по-видимому, с самого начала не было никакого плана. В своих ранних сообщениях, касающихся магазина Silk Road, он поочередно использовал свой настоящий адрес электронной почты и псевдоним.

Как видите, в современном мире очень сложно использовать Интернет, не оставляя следов своей подлинной личности.

Глава 16

ОСВОЕНИЕ ИСКУССТВА БЫТЬ НЕВИДИМЫМ

К этому моменту вы, вероятно, задумались о своем уровне опыта и о том, насколько легко (или сложно) вам будет сохранять конфиденциальность в Интернете. Или спрашиваете себя, насколько далеко вы готовы зайти и насколько вам вообще это нужно. В конце концов, вы можете не обладать государственной тайной! Однако вы можете участвовать в судебной тяжбе со своим бывшим супругом. Или иметь разногласия со своим боссом. Вы можете общаться с другом, который все еще находится в контакте с терроризирующим его членом семьи. Кроме того, вы можете захотеть скрыть некоторые свои действия от адвоката по гражданским делам. Существует множество совершенно безобидных причин, по которым вам может понадобиться общаться с другими людьми через Интернет или использовать сеть и прочие технологии анонимно. Итак…

Какие шаги мне нужно предпринять для обеспечения конфиденциальности? Как много времени это займет? И сколько это будет стоить?

Если к настоящему времени вы еще не вполне это поняли, поясню: чтобы быть невидимым в Интернете, вам необходимо создать отдельную личность, совершенно не связанную с вами. В этом и заключается смысл анонимности. В остальное время вам также необходимо всеми силами отделять свою реальную жизнь от этой анонимной личности. Я имею в виду, что вам нужно приобрести несколько отдельных устройств, которые вы будете использовать только тогда, когда вам необходимо обеспечить анонимность. И это может дорого стоить.

Чтобы быть невидимым в Интернете, вам необходимо создать отдельную личность, совершенно не связанную с вами. В этом и заключается смысл анонимности. В остальное время вам также необходимо всеми силами отделять свою реальную жизнь от этой анонимной личности. Я имею в виду, что вам нужно приобрести несколько отдельных устройств, которые вы будете использовать только тогда, когда вам необходимо обеспечить анонимность. И это может дорого стоить.

Например, вы можете использовать свой существующий ноутбук и создать на нем то, что называется виртуальной машиной. Виртуальная машина — это программа, эмулирующая аппаратное обеспечение компьютера, например VMware Fusion. В виртуальной машине вы можете загрузить лицензионную копию ОС Windows 10 и задать нужный объем оперативной памяти, дискового пространства и т. д. Тому, кто наблюдает за вами через Интернет, будет казаться, что вы используете компьютер под управлением операционной системы Windows 10, когда на самом деле вы используете компьютер Mac.

Профессиональные исследователи в сфере информационной безопасности используют виртуальные машины постоянно, легко создавая и уничтожая их. Однако даже профессионалы могут допустить утечку данных. Например, работая в своей виртуальной машине с операционной системой Windows 10, вы можете случайно проверить свою личную электронную почту. Теперь эту виртуальную машину можно связать с вами лично.

Таким образом, первым шагом при обеспечении анонимности является покупка отдельного ноутбука, который вы будете использовать только для осуществления анонимных действий в Интернете. Как мы видели, стоит вам на секунду забыться и, скажем, проверить свою личную электронную почту на этом компьютере, и игра в анонимность будет окончена. Я рекомендую приобрести недорогой ноутбук под управлением операционной системы Windows (лучше с Linux, если вы умеете использовать эту систему). Причина, по которой я не рекомендую Macbook Pro, заключается в его высокой стоимости по сравнению с Windows-машиной.

Ранее я рекомендовал приобрести второй ноутбук, хромбук, предназначенный только для использования онлайн-банкинга. Другим вариантом получения доступа к этому сервису является использование планшета iPad. Вы должны зарегистрировать учетную запись Apple ID, используя свой адрес электронной почты/пароль и банковскую карту или купив подарочную карту iTunes. Однако поскольку данное устройство предназначено только для безопасного получения доступа к сервису онлайн-банкинга, обеспечение невидимости не является приоритетом.

Однако если ваша цель заключается в обеспечении невидимости, то хромбук — это не лучшее решение, поскольку он не предоставит вам той гибкости, какая свойственна ноутбуку под управлением операционной системы Windows или некоторых представителей семейства Linux, например Ubuntu. Операционная система Windows 10 также допустима при условии, что вы не станете регистрировать учетную запись Microsoft. Вам не следует допускать формирование какой бы то ни было связи между своим компьютером и корпорацией Microsoft.

Вам следует приобрести новый ноутбук за наличные в обычном магазине, а не через Интернет, чтобы эту покупку сложнее было связать с вами. Помните, что ваш новый ноутбук оснащен беспроводной сетевой картой с уникальным MAC-адресом. Нельзя допускать, чтобы кто-либо связал

это оборудование с вами в случае утечки вашего реального MAC-адреса. Например, если вы включите ноутбук, находясь в кофейне Starbucks, система постарается найти любые беспроводные сети, к которым она «подключалась» раньше. Наличие поблизости оборудования, регистрирующего такие пробные запросы, может привести к определению вашего реального MAC-адреса. Одна из проблем заключается в том, что правительство может каким-то образом отследить вашу покупку ноутбука в случае существования какой-либо связи между MAC-адресом вашей сетевой карты и серийным номером вашего компьютера. При этом федералам нужно будет всего лишь выяснить, кто купил конкретный компьютер, чтобы вас идентифицировать, что, вероятно, не составит труда.

Вы должны установить операционную систему Tails и Tor Browser и использовать их вместо операционной системы и браузера, установленных по умолчанию.

Не авторизуйтесь на сайтах или в приложениях, используя свои реальные личные данные. Вам уже известны риски, обусловленные легкостью отслеживания людей и компьютеров через Интернет. Как я говорил, использование сайтов или учетных записей от своего реального имени — грубейший просчет, поскольку банки и другие сайты обычно используют систему распознавания устройств по их цифровым отпечаткам для предотвращения мошенничества. Не исключено, что они смогут идентифицировать ваш компьютер, если вы когда-либо зайдете на тот же сайт анонимно.

На самом деле, лучше всего отключить свой беспроводной маршрутизатор, прежде чем запускать анонимный ноутбук у себя дома. Ваш провайдер может узнать MAC-адрес вашего анонимного ноутбука, когда вы подключитесь к домашнему маршрутизатору (если, конечно, у провайдера есть доступ к нему). Лучше приобрести для дома собственный маршрутизатор, чтобы иметь над ним полный контроль и чтобы провайдер не смог получить доступ к списку MAC-адресов устройств, подключенных к вашей локальной сети. Таким образом, провайдер будет видеть только MAC-адрес вашего маршрутизатора, что не представляет для вас никакого риска.

То, что вам нужно, — это правдоподобное отрицание. Ваши соединения должны быть многократно переадресованы, чтобы следователю было очень сложно связать их с одним человеком, не говоря уже о вас лично. Находясь в бегах, я допустил ошибку. Я неоднократно подключался к модемам интернет-провайдера Netcom с помощью сотового телефона, чтобы замаскировать свое физическое местоположение. Поскольку я находился в одном и том же месте, обнаружить меня можно было простым методом радиопеленгации после определения базовой станции сотовой связи, используемой моим сотовым телефоном. Это позволило моему противнику (Цутому Симомура) установить мое местоположение и передать его ФБР.

Это означает, что вам никогда не следует использовать свой недорогой ноутбук дома. Никогда. Поэтому приобретите ноутбук и запретите себе с его помощью проверять личную электронную почту, обновления в Facebook и даже местный прогноз погоды.

Другой проверенный способ, с помощью которого за вашими действиями в Интернете можно наблюдать, заключается в отслеживании ваших финансовых транзакций. Вам предстоит кое-что оплатить, поэтому прежде чем отправляться со своим анонимным компьютером на поиск публичной точки доступа, анонимно приобретите несколько подарочных карт. Поскольку у киоска или прилавка каждого магазина, торгующего подарочными картами, вероятно, установлены камеры видеонаблюдения, вам следует проявить особую осторожность. Не стоит покупать их самостоятельно. Лучше нанять для этого случайного прохожего, а самому подождать на безопасном расстоянии.

Но как это сделать? Вы можете подойти к кому-нибудь на парковке, как это сделал я, и сказать, что ваша бывшая жена работает в этом магазине и вы не хотите с ней встречаться, или придумайте другую правдоподобную причину. Например, что у нее есть судебный приказ, запрещающий вам приближаться к ней. Кому-то достаточно веской причиной покажутся несколько купюр наличными.

Теперь, когда мы нашли человека, готового зайти в магазин и купить для нас несколько подарочных карт, возникает вопрос, какие именно карты ему следует купить? Я рекомендую приобрести несколько предоплаченных карт номиналом 100 долларов. Не покупайте многоразовые банковские карты, поскольку в соответствии с положениями «Патриотического акта» вы должны будете предоставить свои персональные данные при их активации. Такие покупки требуют предоставления вашего настоящего имени, адреса, даты рождения и номера социального страхования, которые будут соответствовать информации в кредитных бюро. Предоставление вымышленного имени или чужого номера социального страхования является нарушением закона и, вероятно, не стоит того, чтобы рисковать.

Я рекомендую приобрести несколько предоплаченных карт номиналом 100 долларов. Не покупайте многоразовые банковские карты, поскольку в соответствии с положениями «Патриотического акта» вы должны будете предоставить свои персональные данные при их активации. Такие покупки требуют предоставления вашего настоящего имени, адреса, даты рождения и номера социального страхования, которые будут соответствовать информации в кредитных бюро. Предоставление вымышленного имени или чужого номера социального страхования является нарушением закона и,

вероятно, не стоит того, чтобы рисковать.

Мы ведь просто хотим стать невидимыми в Интернете, а не нарушить закон.

Я рекомендую приобрести с помощью посредника подарочную карту Vanilla Visa или Vanilla MasterCard номиналом 100 долларов в сети аптек, магазинов 7-Eleven, Walmart или в супермаркете. Они часто служат в качестве подарков и могут использоваться как обычные банковские карты. Для их покупки не нужно предоставлять какие-либо личные данные. И их можно приобрести анонимно за наличные. Если вы живете в Евросоюзе, вам следует анонимно заказать физическую банковскую карту на сайте **viabuy.com**. В Европе эти карты могут быть доставлены в почтомат, откуда их можно забрать, не предоставляя удостоверения личности. Как я понимаю, в этом случае вам высылается PIN-код, с помощью которого можно открыть ячейку почтомата, чтобы анонимно забрать карты (при условии отсутствия камеры слежения).

Итак, где вы можете использовать свой новый ноутбук и анонимно приобретенные предоплаченные карты?

Благодаря появлению недорогих запоминающих устройств провайдеры бесплатных услуг беспроводной связи могут хранить записи с камер видеонаблюдения на протяжении многих лет. Следователь может относительно легко получить этот материал и поискать на нем подозрительных лиц. Он также может проверить в журналах провайдера MAC-адреса, которые были зарегистрированы в бесплатной сети во время вашего посещения, и сравнить их с вашим MAC-адресом. Именно поэтому так важно менять MAC-адрес при каждом подключении к бесплатной сети Wi-Fi. Вам следует найти место, находящееся по соседству с тем, где предоставляется бесплатная услуга Wi-Fi. Например, по соседству с кофейней Starbucks (или другим учреждением, предоставляющим бесплатный доступ в Интернет) может находиться китайский ресторан. Сядьте за стол у стены, примыкающей к помещению с бесплатной сетью. При этом скорость соединения может оказаться меньше, однако вы обеспечите себе относительную анонимность (по крайней мере, до тех пор, пока следователь не начнет просматривать материал с камер видеонаблюдения, установленных поблизости).

Ваш MAC-адрес, скорее всего, будет сохранен в журнале провайдера после вашего подключения к бесплатной сети. Помните любовницу генерала Дэвида Петреуса? Помните, как дата и время ее регистрации в отеле совпали с появлением MAC-адреса ее компьютера в сети этого отеля? Не допускайте того, чтобы простые ошибки ставили под угрозу вашу анонимность. Не забывайте менять свой MAC-адрес каждый раз при подключении к публичной сети Wi-Fi.

Пока все кажется довольно простым. Вам нужно приобрести отдельный ноутбук для осуществления анонимных действий. Также анонимно вам следует приобрести несколько подарочных карт. Вы должны найти сеть Wi-Fi, к которой вы можете получить доступ из соседнего помещения, чтобы не попасть в объектив камеры видеонаблюдения. Кроме того, вам следует менять свой MAC-адрес каждый раз при подключении к бесплатной беспроводной сети.

Разумеется, это еще далеко не все. Мы только начинаем.

Вы также можете нанять еще одного человека для совершения более важной покупки — персональной точки доступа. Как я уже упоминал, ФБР удалось меня поймать из-за того, что для подключения к находящимся в разных частях мира системам я использовал свой сотовый телефон и модем. Со временем мое местоположение удалось установить из-за того, что мой сотовый телефон использовал одну и ту же базовую станцию. После этого следователи могли легко применить метод радиопеленгации для нахождения приемопередатчика (моего сотового телефона). Вы можете избежать этого, наняв кого-нибудь для покупки в местном магазине Verizon (AT&T или T-Mobile) персональной точки доступа, позволяющей подключаться к Интернету через сотовую связь. Так у вас будет собственная локальная точка доступа к Интернету, что избавит вас от необходимости пользоваться публичной сетью Wi-Fi. Самое главное — никогда не использовать персональную точку доступа в одном и том же месте на протяжении длительного времени, если вы хотите сохранить анонимность.

В идеале человек, которого вы нанимаете для покупки устройства, не должен видеть номерной знак вашего автомобиля или иметь возможность идентифицировать вас каким-либо иным способом. Дайте ему наличные: 200 долларов на покупку, а затем еще 100 долларов, когда он вернется с устройством. Оператор сотовой связи продаст ему персональную точку доступа, не содержащую никакой опознавательной информации. Кроме того, вы можете заодно попросить приобрести для вас несколько пополняемых карт. Конечно, есть риск, что человек просто исчезнет с вашими деньгами, однако ради обеспечения анонимности на него стоит пойти. Позднее вы сможете пополнить баланс этого устройства с помощью биткойнов.

Теперь, когда у вас есть анонимно приобретенная портативная точка доступа, очень важно, чтобы, как в случае с ноутбуком, вы никогда, никогда, никогда не включали ее дома. Каждый раз при включении она связывается с ближайшей базовой станцией оператора сотовой связи. Вам не

нужно, чтобы в файле журнала оператора сотовой связи появился адрес вашего дома, офиса или любого другого места, которое вы часто посещаете.

Кроме того, никогда не включайте свой личный телефон или ноутбук там, где работает ваш анонимный ноутбук, одноразовый телефон или анонимная точка доступа. Это очень важно. Любая запись, которая позднее может связать вашу подлинную личность с анонимной, лишает смысла всю операцию.

Теперь, вооружившись предоплаченными подарочными картами и персональной точкой доступа с предоплатным тарифным планом, приобретенными анонимно двумя совершенно разными людьми, которые не смогут идентифицировать вас при проведении опознания в полиции, вы почти готовы. Почти.

С этого момента вам следует использовать Tor Browser для регистрации и получения доступа ко всем учетным записям в Интернете, поскольку эта программа постоянно меняет ваш IP-адрес.

Для начала необходимо создать несколько анонимных учетных записей электронной почты, используя сеть Tor. Этого-то Росс Ульбрихт и не сделал. Как мы видели в предыдущей главе, он неоднократно использовал свой личный адрес электронной почты (), развивая свой бизнес Silk Road в Даркнете. Эти непреднамеренные пересечения между пользователем с ником Dead Pirate Roberts и Россом Ульбрихтом позволили следователям доказать, что эти два имени относятся к одному и тому же человеку.

Для предотвращения возможных злоупотреблений большинство почтовых сервисов, например, Gmail, Hotmail, Outlook и Yahoo! требуют верификации по номеру сотового телефона. Это означает, что вы должны предоставить номер своего телефона, на который в процессе регистрации поступит текстовое сообщение для подтверждения вашей личности.

При наличии одноразового телефона вы все равно можете использовать перечисленные выше коммерческие сервисы. Однако этот телефон и пополняемые карты следует приобрести за наличные через подставное лицо, связь которого с вами невозможно будет установить. Кроме того, этот одноразовый телефон нельзя использовать рядом с другими вашими устройствами, оснащенными средствами сотовой связи. Свой личный телефон следует оставлять дома.

Для покупки биткойнов через Интернет вам понадобятся, по крайней мере, два анонимно созданных адреса электронной почты и два биткойн-кошелька. Итак, как же создать анонимную учетную запись электронной почты, как это сделали Эдвард Сноуден и Лора Пойтрас?

В ходе своих исследований мне удалось создать учетную запись электронной почты на сервисах **protonmail.com** и **tutanota.com** с помощью Tor Browser, не проходя никакой процедуры верификации. Ни один из этих небольших провайдеров электронной почты не потребовал от меня подтвердить свою личность при регистрации. Вы можете провести собственное исследование, проверив, требует ли тот или иной сервис электронной почты предоставления номера сотового телефона при регистрации. Вы также можете узнать, сколько информации необходимо предоставить сервису для создания новой учетной записи. Еще одним сервисом безымянной электронной почты является **fastmail.com**, функционал которого не так богат, как у Gmail, но который, будучи платным, не охотится за пользовательскими данными и не показывает рекламные объявления.

Теперь у нас есть ноутбук с установленными Tor Browser и Tails, одноразовый телефон, несколько анонимных предоплаченных подарочных карт, а также анонимная точка доступа с анонимно приобретенным тарифным планом. Однако мы все еще не готовы. Для сохранения конфиденциальности нам нужно преобразовать наши анонимно приобретенные предоплаченные подарочные карты в биткойны.

В главе 6 мы говорили о такой виртуальной валюте, как биткойн. Сами по себе биткойны не обеспечивают анонимность. Их можно отследить по блокчейну до того, кто инициировал покупку, и таким же образом можно отслеживать все последующие покупки. Таким образом, сам по себе биткойн не позволит скрыть вашу личность. Нам придется провести денежные средства через механизм анонимизации: мы конвертируем предоплаченные подарочные карты в биткойны, а затем «отделим» их от нашей личности с помощью специального сервиса. Это позволит получить анонимные биткойны, которые мы будем использовать для проведения будущих платежей. Например, «анонимные» биткойны понадобятся нам для оплаты услуги VPN, а также пополнения баланса нашей мобильной точки доступа или одноразового телефона.

Используя сеть Tor, вы можете настроить исходный биткойн-кошелек на сайте **paxful.com** или на другом аналогичном сервисе. Некоторые сайты позволяют обменять на биткойны предоплаченные подарочные карты вроде упомянутых ранее Vanilla Visa и Vanilla MasterCard.

Недостатком является огромная цена такой услуги, составляющая минимум 50 %.

Сайт **paxful.com** напоминает маркет eBay, который просто соединяет вас с покупателями и продавцами биткойнов.

Очевидно, анонимность — это дорогое удовольствие. Чем меньше идентифицирующей информации вы предоставляете при проведении транзакции, тем больше вам придется за нее заплатить. Это имеет смысл: люди, продающие биткойны, подвергаются огромному риску, не проверяя вашу личность. Я смог обменять на биткойны анонимно приобретенные подарочные карты Vanilla Visa по ставке 1,70 доллара за доллар, что, конечно, возмутительно, но необходимо для обеспечения анонимности.

Я уже упомянул, что сами по себе биткойны не являются анонимными. Например, в результате проведенной мной операции появилась запись о том, что я обменял несколько предоплаченных подарочных карт на некоторое количество биткойнов. Следователь может установить связь между моими биткойнами и подарочными картами.

Однако есть способы отмывания биткойнов, позволяющие еще сильнее запутать любые следы, ведущие ко мне.

Отмывание денег — это то, чем преступники занимаются все время. Чаще всего эти механизмы используются при торговле наркотиками, а также в финансовых преступлениях, совершаемых «белыми воротничками». При отмывании вы скрываете первоначального собственника средств, зачастую отправляя деньги в банки других стран, где действуют строгие законы о конфиденциальности. Оказывается, что-то подобное можно делать и с виртуальной валютой.

Существуют сервисы, называемые биткойн-миксерами, которые смешивают биткойны из разных источников, в результате чего их стоимость остается прежней, но теперь следы от них ведут ко многим владельцам. Это затрудняет последующее определение того, какой из владельцев совершил ту или иную покупку. Однако вам следует быть чрезвычайно осторожным, поскольку в Интернете много мошенников.

Я рискнул — нашел сервис анонимизации и внес дополнительную плату за проведение транзакции. Я действительно получил нужное мне количество биткойнов. Однако подумайте вот о чем: теперь этому сервису известен один из моих анонимных адресов электронной почты, а также два адреса биткойн-кошельков, используемых при проведении транзакции. Чтобы еще больше запутать следы, я сделал так, чтобы биткойны были отправлены на второй биткойн-кошелек, зарегистрированный с использованием другой цепочки узлов Tor, которая послужила промежуточным звеном между мной и сайтом, который я хотел посетить. Теперь транзакция оказалась достаточно запутанной, что весьма затруднило бы в дальнейшем установление того факта, что эти два биткойн-кошелька принадлежат одному и тому же человеку. Разумеется, сервис по отмыванию биткойнов может предоставить оба биткойн-кошелька третьей стороне. Именно поэтому так важно приобретать предоплаченные подарочные карты.

После использования подарочных карт для покупки биткойнов не забудьте избавиться от пластиковых карточек (не выбрасывайте их в мусорную корзину у себя дома). Я рекомендую воспользоваться для этого шредером с перекрестной резкой, рассчитанным на пластиковые карты, после чего выбросить куски в мусорный бак подальше от дома или офиса. После получения отмытых биткойнов вы можете зарегистрироваться на сервисе VPN, для которого конфиденциальность пользователя является приоритетом. Лучшая политика при попытке обеспечить анонимность заключается в том, чтобы не доверять VPN-провайдеру, особенно тому, который утверждает, что не хранит никаких журналов. Скорее всего, он выдаст ваши данные, если этого потребуют правоохранительные органы или спецслужбы.

Например, я не могу представить, чтобы какой-либо VPN-провайдер не имел возможности устранить проблемы в собственной сети. Для устранения неполадок требуется ведение нескольких журналов; например, с помощью журналов соединений можно установить связь между клиентами и их IP-адресами.

Итак, поскольку даже лучшим из этих провайдеров нельзя доверять, мы оплатим услугу VPN через Tor Browser, используя биткойны, прошедшие через миксер, чтобы их было невозможно связать с вами. Я рекомендую ознакомиться с условиями обслуживания и политикой конфиденциальности VPN-провайдера и на основании этого выбрать наилучший вариант. Вы не найдете идеального варианта, только достаточно хороший. Помните о том, что вы не можете доверить никакому провайдеру обеспечение вашей анонимности. Вы должны позаботиться об этом самостоятельно, понимая, что одна-единственная ошибка может выдать вашу настоящую личность.

Теперь, когда у вас есть автономный ноутбук с Tor Browser или Tails, подключенной услугой VPN, оплаченной отмытыми биткойнами через анонимно купленную точку доступа, а также еще некоторое количество отмытых биткойнов, можно сказать, что вы выполнили самую легкую часть работы, связанную с настройкой. На это вам пришлось потратить от 200 до 500 долларов, однако все эти компоненты были приобретены достаточно случайным образом, так что их нелегко будет

связать с вами. Теперь приступим к сложной части — поддержанию достигнутой анонимности.

Результат проделанной работы может быть мгновенно потерян, если вы активируете анонимную точку доступа дома или используете свой персональный сотовый телефон, планшет или любое интернет-устройство, связанное с вашей реальной личностью, в месте использования вашей анонимной личности. Достаточно одного вашего промаха для того, чтобы следователь-криминалист смог установить факт вашего присутствия в конкретном месте, проанализировав журналы оператора сотовой связи. Обнаружение взаимосвязи между анонимным доступом и регистрацией вашего сотового устройства в том же месте может привести к разоблачению вашей реальной личности.

Я уже привел несколько примеров того, как это может произойти.

Если ваша конфиденциальность будет поставлена под угрозу, а вам потребуется произвести другие анонимные действия, то придется пройти весь процесс еще раз — безвозвратно удалить и снова установить операционную систему на свой анонимный ноутбук, зарегистрировать новые анонимные учетные записи электронной почты и биткойн-кошельки, купить другую анонимную точку доступа. Напомню, что Эдвард Сноуден и Лора Пойтрас, уже имея анонимные учетные записи электронной почты, зарегистрировали дополнительные анонимные аккаунты электронной почты для общения исключительно друг с другом. Это необходимо только в том случае, если вы считаете, что изначально обеспеченная вами анонимность поставлена под угрозу. В противном случае вы можете использовать Tor Browser (после перекоммутации) через анонимную точку доступа и VPN-сервис, позволяющие получить доступ к Интернету от другого имени.

Разумеется, то, в какой степени вы последуете этим рекомендациям, зависит от вас.

Даже если вы будете следовать моим рекомендациям, существует вероятность того, что кто-то на другом конце вас опознает. Каким образом?

По тому, как вы печатаете текст.

Даже если вы будете следовать моим рекомендациям, существует вероятность того, что кто-то на другом конце вас опознает. Каким образом? По тому, как вы печатаете текст.

Существует довольно много исследований, в которых основное внимание уделяется выбору конкретных слов, которые используют люди при написании писем или комментариев в социальных сетях. По конкретным словам исследователи часто способны определить пол и этническую принадлежность автора. Однако ничего более конкретного они сказать не могут.

Но так ли это?

Во время Второй мировой войны британское правительство установило по всей стране множество станций для перехвата сигналов, посылаемых немецкими военными. Успехи, позволившие союзникам расшифровать эти сообщения, были достигнуты несколько позже, в Блетчли-Парк — Правительственной школе кодирования и шифрования, где был взломан код немецкой шифровальной машины «Энигма». Чуть ранее исследователи из Блетчли-Парк, перехватывающие немецкие телеграфные сообщения, научились выявлять уникальные характеристики отправителя, основываясь на временных интервалах между точками и тире. Например, они могли определить момент выхода в сеть новых телеграфистов, которым даже начали давать имена.

Как простые точки и тире могли выдать стоящих за ними людей?

Дело в том, что временной интервал между нажатием двух клавиш можно измерить. В дальнейшем этот метод получил название «Кулак отправителя». Разных операторов, использующих азбуку Морзе, можно идентифицировать по их уникальным «кулакам». Телеграф разрабатывался не для этого (в конце концов, важно *содержание* сообщения, а не то, кто конкретно его отправил), однако в данном случае возможность определения уникальных нажатий клавиш явилась интересным побочным эффектом.

Сегодня благодаря достижениям в области цифровых технологий электронные устройства позволяют фиксировать измеряемые в наносекундах различия во временных интервалах, с которыми разные люди нажимают клавиши на клавиатурах компьютеров, включая не только продолжительность удерживания клавиши в нажатом состоянии, но и то, сколько времени прошло до нажатия следующей клавиши. Это позволяет определить, кто набирает текст быстро, а кто медленно. Это в сочетании с выбором слов может многое рассказать об авторе анонимного сообщения.

И это — серьезная проблема, поскольку даже если вы обеспечили анонимность своего IP-адреса, то сайт, на который вы зашли, все равно может вас опознать, но не по какой-то технической причине, а из-за того, что присуще только вам как человеку. Для этого используется так называемый поведенческий анализ.

Допустим, владельцы сайта, к которому вы получили доступ через сеть Tor, решают отследить производимые вами нажатия клавиш. Возможно, они являются злоумышленниками и хотят больше о вас узнать. А может быть, они сотрудничают с правоохранительными органами.

Многие финансовые организации уже используют анализ динамики нажатия клавиш для дополнительной аутентификации владельцев учетных записей. Таким образом, если у кого-то будет ваше имя пользователя и пароль, он или она не сможет подделать ваш клавиатурный почерк. Это хорошо, если вы хотите быть узнанным в Интернете. А если вам это не нужно?

Поскольку анализ динамики нажатия клавиш так легко реализовать, исследователи Пер Торсхайм и Пол Мур создали плагин для браузера Chrome под названием Keyboard Privacy. Этот плагин кэширует ваши отдельные нажатия клавиш, а затем воспроизводит их с различными временными интервалами. Идея состоит в добавлении элемента случайности в ваш клавиатурный почерк для обеспечения анонимности при работе в Интернете. Этот плагин позволяет дополнительно замаскировать ваши анонимные действия в сети.

Как вы уже убедились, разделить вашу реальную жизнь и анонимную жизнь в Интернете возможно, но это требует постоянной бдительности. В предыдущей главе я описал несколько впечатляющих промахов в сохранении анонимности. Это были славные, но кратковременные попытки обеспечить свою невидимость.

Что касается Ульбрихта, то он не очень тщательно разработал свое альтер-эго и иногда использовал свой реальный адрес электронной почты вместо анонимного, особенно в самом начале. С помощью расширенного поиска средствами Google следователь смог собрать достаточно информации для того, чтобы раскрыть личность таинственного владельца сайта Silk Road.

Теперь разберемся с Эдвардом Сноуденом и другими подобными ему людьми, которые обеспокоены слежкой, ведущейся за ними одним или несколькими правительственными учреждениями. Например, у Сноудена есть учетная запись в Twitter. Как и у многих других людей, стремящихся сохранить конфиденциальность, — как еще они могут провести острое обсуждение в Интернете. Есть две возможные причины, объясняющие, как этим людям удается оставаться «невидимыми».

Они не находятся под активным наблюдением. Возможно, правительство или правительственное агентство точно знает, где находятся его цели, но ему нет до них никакого дела. Если они не нарушают никаких законов, кто обратит внимание на их кратковременную потерю бдительности. Они могут заявить, что используют Tor только для анонимной почты, а потом использовать эту же учетную запись для совершения покупок на сервисе Netflix.

Они находятся под наблюдением, но не могут быть арестованы. Я думаю, этот сценарий очень хорошо применим к Сноудену. Возможно, в какой-то момент он допустил оплошность, и теперь его повсюду активно выслеживают, правда он живет в России. А у России нет реальной причины для его ареста и депортации в Соединенные Штаты.

Я сказал, что эти люди допустили промах. Если вы не обладаете сверхъестественным вниманием к деталям, то вам будет очень трудно жить двумя жизнями. Я знаю. Я пытался. Я потерял бдительность, когда использовал для доступа к компьютерам сотовую сеть в одном и том же месте.

Среди специалистов по информационной безопасности принято считать, что настойчивый злоумышленник может достичь успеха при наличии достаточного количества времени и ресурсов. Я всегда его достигаю при проведении проверки системы безопасности моих клиентов. По большому счету обеспечение безопасности сводится к созданию достаточного количества препятствий, чтобы атакующий отказался от дальнейших попыток и выбрал другую цель.

Большинству из нас бывает необходимо скрыться лишь на короткое время. Например, от шефа, который хочет нас уволить, от бывшего супруга, чьи адвокаты ищут то, что можно было бы использовать против нас, или от жуткого сталкера, увидевшего нашу фотографию на Facebook и решившего нас преследовать. Какова бы ни была причина, данные мной рекомендации позволят обеспечить вашу невидимость на время, необходимое для выхода из неприятной социальной ситуации.

Обеспечение анонимности в современном цифровом мире — это большая работа, требующая постоянной бдительности. У каждого человека свои стандарты конфиденциальности: кому-то нужно защитить свои пароли и скрыть личные документы от коллег, кому-то — скрыться от назойливого поклонника, а кому-то — скрыться от АНБ, потому что он располагает множеством эксплойтов к уязвимостям нулевого дня, которые агентство с удовольствием использовало бы против террористических ресурсов.

Ваши индивидуальные потребности будут определять действия, которые необходимо предпринять для поддержания желаемого уровня анонимности, начиная от установки надежных паролей и осознания угроз, связанных с использованием офисного принтера, и заканчивая описанными выше

рекомендациями, призванными значительно усложнить следователю задачу по установлению вашей подлинной личности.

Вообще, всем нам не помешает ознакомиться со способами сведения к минимуму наших цифровых отпечатков пальцев в современном мире. Нам следует подумать, прежде чем публиковать фотографию, на заднем плане которой виден наш адрес. Или прежде чем предоставлять настоящую дату рождения и другую персональную информацию в наших профилях в социальных сетях. Или прежде чем путешествовать по Всемирной паутине без использования расширения HTTPS Everywhere. Или прежде чем совершать конфиденциальные вызовы и отправлять текстовые сообщения без использования инструмента сквозного шифрования, например Signal. Или прежде чем общаться со своим врачом с помощью мессенджера AOL, MSN Messenger или Google Talk без протокола OTR. Или прежде чем отправлять конфиденциальное электронное письмо без применения шифрования PGP или GnuPG.

Мы можем заранее подумать о нашей информации и осознать, что, даже если наши действия кажутся нам безобидными, публикуя фотографию, забывая сменить пароли, установленные по умолчанию, используя рабочий телефон для совершения личного звонка или создавая учетную запись Facebook для наших маленьких детей, мы принимаем решения, последствия которых будем ощущать всю жизнь. Поэтому действовать нам следует, исходя из этих соображений.

Эта книга посвящена тому, как работать в Интернете, сохраняя при этом свою драгоценную конфиденциальность. Всем, начиная с самого далекого от техники пользователя и заканчивая экспертом по информационной безопасности, следует стремиться овладеть искусством, которое с каждым днем становится все более актуальным, — искусством быть невидимым.

Благодарности

Эта книга посвящена моей любящей матери, Шелли Яффе, и моей бабушке Ребе Вартанян, которые многим жертвовали для меня на протяжении всей моей жизни. В какой бы ситуации я ни оказался, мои мама и бабушка всегда поддерживали меня, особенно в трудные времена. Эта книга не была бы написана без поддержки моей прекрасной семьи, которая всегда дарила мне столько безусловной любви.

15 апреля 2013 года моя мать скончалась после долгой борьбы с раком легких. Это произошло после многих лет страданий и попыток оправиться от последствий химиотерапии. Я помню несколько хороших дней после проведения ужасных процедур, используемых современной медициной для борьбы с этим видом онкологии. Как правило, у подобных пациентов остается очень мало времени — обычно болезнь одолевает их за считанные месяцы. Я очень благодарен за то время, которое я смог провести с ней, пока она сражалась с этой ужасной болезнью. И я очень счастлив, что меня вырастила такая любящая и преданная мать, которую я также считаю своим лучшим другом. Моя мама была удивительным человеком, и я невероятно скучаю по ней.

7 марта 2012 года моя бабушка неожиданно скончалась во время лечения в госпитале Sunrise в Лас-Вегасе. Наша семья ожидала, что она вернется домой, но этого так и не произошло. На протяжении последних нескольких лет жизни моя бабушка постоянно переживала из-за болезни моей матери. Мне ее ужасно не хватает, я бы очень хотел разделить с ней радость от этого достижения.

Я надеялся, эта книга принесет много радости моей матери и бабушке и заставит их гордиться тем, что я помогаю людям защитить неприкосновенность своей частной жизни.

Я хотел бы, чтобы мой отец, Алан Митник, и мой брат, Адам Митник, вместе со мной отпраздновали публикацию этой важной книги, посвященной обеспечению невидимости в эпоху, когда шпионаж и слежка стали обычным явлением.

При написании этой книги мне посчастливилось работать с экспертом в сфере информационной безопасности, Робертом Вамоси. Его глубокие познания в области безопасности и писательский талант позволили ему найти интересные истории, провести исследования, а также сформулировать предоставленную мной информацию так, чтобы ее мог понять любой далекий от техники человек. Я должен отдать должное Робу, который проделал потрясающую работу. Честно говоря, я не смог бы завершить этот проект без него.

Я очень хочу поблагодарить тех невероятно преданных своему делу людей, которые помогли мне рассказать о моей профессиональной карьере. Мой литературный агент Дэвид Фьюгейт из LaunchBooks помог заключить контракт на эту книгу, а также выступал в качестве посредника между мной и издательством Little, Brown. Концепция книги «Искусство быть невидимым» была разработана Джоном Рафузе из компании 121 Minds, который является моим агентом, занимающимся организацией моих выступлений, кроме того, он также отвечает за стратегическое развитие бизнеса моей компании. По собственной инициативе Джон сделал мне интригующее предложение, касающееся написания книги, а также предоставил макет обложки. Он настоятельно рекомендовал мне написать эту книгу, чтобы помочь жителям всего мира защитить свои права на частную жизнь от посягательств Большого Брата и Больших Данных. Джон — потрясающий человек.

Я благодарен за возможность работать над этим захватывающим проектом с издательством Little, Brown. Хочу сказать спасибо своему редактору, Джону Парсли, за всю проделанную им работу и советы. Спасибо, Джон.

Я также благодарю своего друга, Микко Хиппонена, главного исследователя компании F-Secure, за то, что он потратил свое драгоценное время на написание предисловия к этой книге. Микко — очень уважаемый эксперт в сфере безопасности и обеспечения конфиденциальности данных. Он занимается исследованием вредоносного программного обеспечения уже более двадцати пяти лет.

Кроме того, я хотел бы поблагодарить Томи Туоминена из компании F-Secure за то, что он нашел в своем плотном графике время на техническую редактуру рукописи и помог найти ошибки и упущения.

Об авторе

Кевин Митник — герой бесчисленного количества статей и передач по всему миру. Его команда, занимающаяся тестированием на проникновение, пользуется большим уважением и предоставляет свои услуги ведущим корпорациям и правительствам мира. Клиентами его компании, Mitnick Security Consulting LLC, стали десятки входящих в рейтинг Fortune 500 компаний по всему миру. Митник — автор таких бестселлеров, как «Призрак в сети», «Искусство вторжения» и «Искусство обмана». Он живет в Лас-Вегасе и путешествует по миру, выступая в качестве основного докладчика на конференциях, посвященных кибербезопасности.

mitnicksecurity.com

twitter.com/kevinmitnick

Ссылки

Все исходные URL-адреса, приведенные ниже, проверены на момент написания этой книги в июле 2016 года.

Введение

Скачав сотни тысяч засекреченных документов АНБ, Сноуден, который тогда жил на Гавайях, сначала отправился в Гонконг, а затем получил вид на жительство в России. Позже он подавал прошение на проживание в Бразилии и других странах, а также не исключает возможности возвращения в США, если ему гарантируют беспристрастный и честный суд.

reuters.com/article/2011/02/24/idUSN2427826420110224

law.cornell.edu/supct/html/98-93.ZD.html

law.cornell.edu/uscode/text/16/3372

wired.com/2013/06/why-i-have-nothing-to-hide-is-the-wrong-way-to-think-about-surveillance/

Глава 1

apple.com/pr/library/2014/09/02Apple-Media-Advisory.html

anon-ib.com. Примите во внимание, что этот сайт также небезопасен, кроме того, на нем могут находиться изображения оскорбительного содержания.

wired.com/2014/09/eppb-icloud/

justice.gov/usao-mdpa/pr/lancaster-county-man-sentenced-18-months-federal-prison-hacking-apple-and-google-e-mail

arstechnica.com/security/2015/09/new-stats-show-ashley-madison-passwords-are-just-as-weak-as-all-the-rest/

openwall.com/john/

«УМэриБылБарашек123$» после обработки сервисом md5hash-generator.com

news.bbc.co.uk/2/hi/technology/3639679.stm

consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm

mercurynews.com/2014/10/24/warrant-chp-officer-says-stealing-nude-photos-from-female-arrestees-game-for-cops/

arstechnica.com/information-technology/2015/08/new-data-un-covers-the-surprising-predictability-of-android-lock-patterns/

archive.knoxnews.com/news/local/official-explains-placing-david-kernell-at-ky-facility-ep-406501153-358133611.html

wired.com/2008/09/palin-e-mail-ha/

splinternews.com/your-mothers-maiden-name-has-been-a-security-question-s-1793846367

web.archive.org/web/20110514200839/. com/webscout/2008/09/4chans-half-hac.html

commercialappeal.com/news/david-kernell-ut-student-in-palin-email-case-is-released-from-supervisionep-361319081-326647571.html

edition.cnn.com/2010/CRIME/11/12/tennessee.palin.hacking.

case/index.html

symantec.com/connect/blogs/password-recovery-scam-tricks-us-ers-handing-over-email-account-access

techcrunch.com/2016/06/10/how-activist-deray-mckessons-twitter-account-was-hacked/

Глава 2

Если вам интересно, поиском и маркированием изображений, содержащих сцены растления малолетних, занимается организация National Center for Missing and Exploited Children (NCMEC, Национальный центр помощи пропавшим и пострадавшим детям), благодаря чему роботы Google и других поисковых систем распознают подобные изображения, выделяя их среди фотографий непорнографического содержания. dailymail.co.uk/news/article-2715396/Google’s-email-scan-helps-catch-sex-offender-tips-police-indecent-images-children-Gmail-account.html

braingle.com/brainteasers/codes/caesar.php

theintercept.com/2014/10/28/smuggling-snowden-secrets/

Например, см. список здесь: en.wikipedia.org/wiki/Category: Cryptographic_algorithms

Плагин Mailvelope совместим с Outlook.com, Gmail, Почта Yahoo! и некоторыми другими сервисами веб-почты. mailvelope.com

Например, чтобы просмотреть метаданные в аккаунте Gmail, выберите письмо, откройте его, затем щелкните по указывающей вниз стрелке в верхнем правом углу сообщения. Откроется меню (Ответить, Переслать, Фильтровать похожие письма и т. д.), с вариантом **Показать оригинал** (Show Original). Если вы пользуетесь устройством Apple, откройте письмо, затем выберите команду меню **Просмотреть** —> **Сообщение** —> **Все заголовки** (View —> Message —> All Headers). В Yahoo! нажмите кнопку **Дополнительно** (More), затем **Показать сырое сообще**ние (View Raw Message). Аналогичные опции существуют и в других почтовых сервисах.

bbc.com/future/story/20150206-biggest-myth-about-phone-privacy

immersion.media.mit.edu

npr.org/2013/06/13/191226106/fisa-court-appears-to-be-rubber-stamp-for-government-requests

Напечатайте в поисковой строке Google запрос «мой IP-адрес», и увидите свой IP-адрес.

play.google.com/store/apps/details?id=org.torproject.android

wired.com/threatlevel/2014/01/tormail/

theguardian.com/technology/2014/oct/28/tor-users-advised-check-computers-malware

arstechnica.com/security/2014/07/active-attack-on-tor-network-tried-to-decloak-users-for-five-months/

Для настройки браузера Tor на устройстве Raspberry Pi можно воспользоваться специализированным порталом, таким как этот: github.com/grugq/PORTALofPi

skype.com/ru/features/online-number/

newyorker.com/magazine/2007/02/19/the-kona-files

Опять же, вероятно, лучше избегать почты Google или других крупных почтовых сервисов, но я привел этот пример исключительно для наглядности.

Глава 3

Пользователи Android могут отказаться от передачи своих личных данных, войдя в **Настройки** —> **Поиск и сейчас** —> **Учетные записи и конфиденциальность** —> **Совместное использование** (Settings —> Search & Now —> Accounts & privacy —> Commute sharing). У пользователей Apple

отсутствует такая возможность, зато, возможно, будущие версии iOS будут подсказывать оптимальный маршрут, опираясь на местоположение телефона в текущий момент времени.

abc.net.au/news/2015-07-06/nick-mckenzie-speaks-out-about-his-brush-with-the-mafia/6596098

На самом деле вы купите карточку пополнения баланса телефона. Для этого лучше всего пользоваться биткойнами.

washingtonpost.com/news/the-switch/wp/2014/12/18/german-researchers-discover-a-flaw-that-could-let-anyone-listen-to-your-cell-calls-and-read-your-texts/

arstechnica.com/gadgets/2010/12/15-phone-3-minutes-all-thats-needed-to-eavesdrop-on-gsm-call/

latimes.com/local/la-me-pellicano5mar05-story.html# navtype=storygallery

nytimes.com/2008/03/24/business/media/24pellicano.html? pagewanted=all

hollywoodreporter.com/thr-esq/anthony-pellicanos-prison-sentence-vacated-817558

cryptophone. de/en/products/landline/

spectrum.ieee.org/telecom/security/the-athens-affair

bits.blogs.nytimes.com/2007/07/10/engineers-as-counterspys-how-the-greek-cellphone-system-was-bugged/

play.google.com/store/apps/details?id=org.thoughtcrime.securesms itunes.apple.com/ru/app/signal-private-messenger/id874139669?mt=8

Глава 4

caselaw.findlaw.com/wa-supreme-court/1658742.html

courts.mrsc.org/mc/courts/zsupreme/179wn2d/179wn2d0862.htm

komonews.com/news/local/Justices-People-have-right-to-privacy-in-text-messages-247583351.html

democracynow.org/2016/10/26/headlines/project_hemisphere_at_ ts_secret_program_to_spy_on_americans_for_profit

wired.com/2015/08/know-nsa-atts-spying-pact/

espn.go.com/nfl/story/_/id/13570716/tom-brady-new-england-patriots-wins-appeal-nfl-deflategate

bostonglobe.com/sports/2015/07/28/tom-brady-destroyed-his-cellphone-and-texts-along-with/ZuIYu0he05XxEe0mHzwTSK/story.html

DES и AES — это две разные криптографические системы. DES был взломан отчасти потому, что он шифрует данные однократно. При AES происходит трехслойное шифрование, что означает гораздо меньшую степень зависимости от количества бит.

Diskreet больше не применяется.

twitter.com/kevinmitnick/status/346065664592711680, а здесь вы найдете более подробное техническое описание DES с длиной ключа 32 бита: cs.auckland.ac.nz/~pgut001/pubs/norton.txt

theatlantic.com/technology/archive/2014/06/facebook-texting-teens-instagram-snapchat-most-popular-social-network/373043/

pewinternet.org/2015/04/09/teens-social-media-technology-2015

forbes.com/sites/andygreenberg/2014/02/21/whatsapp-comes-under-new-scrutiny-for-privacy-policy-encryption-gaffs/

wired.com/2016/10/facebook-completely-encrypted-messenger-update-now/

privacy.microsoft.com/ru-ru/privacystatement#accessingPersonal Data

eff.org/deeplinks/2011/12/effs-raises-concerns-about-new-aol-instant-messenger-0

wired.com/2007/05/always_two_ther/

venturebeat.com/2016/08/02/hackers-break-into-telegram-revealing-15-million-users-phone-numbers/

csmonitor.com/World/Passcode/2015/0224/Private-chat-app-Telegram — may-not-be-as-secretive-as-advertised

otr.cypherpunks.ca

chatsecure.org

guardianproject.info/apps/chatsecure/

crypto.cat

getconfide.com

Глава 5

techdirt.com/articles/20150606/16191831259/according-to-government-clearing-your-browser-history-is-felony.shtml

cbc.ca/news/trending/clearing-your-browser-history-can-be-deemed-obstruction-of-justice-in-the-u-s -1.3105222

ftpcontent2.worldnow.com/whdh/pdf/Matanov-Khairullozhon-in-dictment.pdf

eff.org/https-everywhere/

tekrevue.com/safari-sync-browser-history/

theguardian.com/commentisfree/2013/aug/01/government-tracking-google-searches

myaccount.google.com/intro/privacy

fastcompany.com/3026698/inside-duckduckgo-googles-tiniest-fiercest-competitor

Глава 6

timlibert.me/pdf/Libert-2015-Health_Privacy_on_Web.pdf

Неофициальное тестирование в процессе работы над этой книгой дало следующие результаты: после того как я ввел в поиск фразу «эпидермофития стоп», расширение Ghostery для браузера Chrome заблокировало 21 запрос от партнеров медицинского центра Mayo Clinic (Клиника Мэйо) и 12 запросов от партнеров сайта WebMD.

Чтобы узнать, какую именно информацию разглашает ваш браузер, посетите сайт browserspy.dk

noscript.net/

crx.dam.io/files/hcdjknjpbnhdoabbngpmfekaecnpajba/1.4.zip Нужно скачать файл, сменить расширение zip на crx и перетащить/активировать на странице chrome://extensions. Режим разработчика должен быть включен.

ghostery.com/products/?utm_source=ghostery.com&utm_ campaign=install_ghostery

Альтернативой абонентскому ящику может быть и пункт выдачи заказов, хотя в некоторых из них требуется предъявлять документ, удостоверяющий личность.

wired.com/2014/10/verizons-perma-cookie/

pcworld.com/article/2848026/att-kills-the-permacookie-stops-tracking-customers-internet-usage-for-now.html

verizonwireless.com/support/unique-identifier-header-faqs/

reputationdefender.com/blog/privacy/how-disable-and-delete-flash-cookies; brighthub.com/computing/smb-security/articles/59530.aspx

en.wikipedia.org/wiki/Samy_Kamkar

github.com/samyk/evercookieventurebeat.com/2015/07/14/consumers-want-privacy-yet-demand-personalization/

businessinsider.com/facebook-will-not-honor-do-not-track-2014-6

chrome.google.com/webstore/detail/disconnect-facebook-pixel/ nnkndeagapifodhlebifbgbonbfmlnfm

facebook.adblockplus.me/

zephoria.com/top-15-valuable-facebook-statistics/

latimes.com/business/la-fi-lazarus-20150417-column.html

propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block#

addons.mozilla.org/en-us/firefox/addon/canvasblocker/

chrome.google.com/webstore/detail/canvasfingerprintblock/ipmjn gkmngdcdpmgmiebdmfbkcecdndc?hl=en-US

trac.torproject.org/projects/tor/ticket/6253

technologyreview.com/s/538731/how-ads-follow-you-from-phone-to-desktop-to-tablet

theintercept.com/2014/10/28/smuggling-snowden-secrets/

Глава 7

computerworld.com/article/2511814/security0/man-used-neighbor-s-wi-fi-to-threaten-vice-president-biden.html

computerworld.com/article/2476444/mobile-security-comcast-xfinity-wifi-just-say-no.html

customer.xfinity.com/help-and-support/internet/disable-xfinity-wifi-home-hotspot/

BitTorrent — это сервис потокового вещания, часть контента для которого предоставляют лица, не являющиеся правообладателями.

blog.privatewifi.com/why-six-strikes-could-be-a-nightmare-for-your-internet-privacy/

Также существуют сети с базовым набором услуг (BSS), которые являются базовыми образующими элементами беспроводной сети LAN стандарта 802.11. Каждой сети с базовым набором услуг (BSS) или с расширенным набором услуг (ESS) присваивается идентификатор набора услуг (Service Set Identifier, SSID).

techspot.com/guides/287-default-router-ip-addresses/

routeripaddress.com/

Узнать MAC-адреса устройств из белого списка можно с помощью инструмента Wireshark, применяющегося для анализа трафика.

pwnieexpress.com/blog/wps-cracking-with-reaver

wired.com/2010/10/webcam-spy-settlement/

telegraph.co.uk/technology/internet-security/11153381/How-hackers-took-over-my-computer.html

blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter.pdf

wired.com/2010/01/operation-aurora/

nytimes.com/2015/01/04/opinion/sunday/how-my-mom-got-hacked.html

arstechnica.com/security/2013/10/youre-infected-if-you-want-to-see-your-data-again-pay-us-300-in-bitcoins/

securityledger.com/2015/10/fbis-advice-on-cryptolocker-just-pay-the-ransom/

Глава 8

Важно отметить, что не во всех странах мира можно свободно подключиться к общественной сети Wi-Fi. Например, в Сингапуре, чтобы пользоваться общественной точкой доступа Wi-Fi за пределами отеля или местного ресторана McDonald’s, нужно зарегистрироваться. Чтобы получить доступ, у местных жителей должен быть сингапурский номер телефона, а туристы обязаны предъявить свой паспорт местным властям.

business.f-secure.com/the-dangers-of-public-wifi-and-crazy-things-people-do-to-use-it/

dnlongen.blogspot.com/2015/05/is-your-home-router-spying-on-you.html

При выборе VPN-сервиса нужно разобраться со множеством моментов. См. torrentfreak.com/anonymous-vpn-service-provider-review-2015-150228/3/

Один из коммерческих VPN-сервисов называется TunnelBear. Он принадлежит канадской компании и совместим с операционными системами Android, iOS и Windows. На сайте сервиса заявлено: «TunnelBear НЕ хранит IP-адреса пользователей, подключившихся к нашему сервису, и поэтому не может идентифицировать пользователей по IP-адресам наших серверов. Кроме того, мы не можем разглашать информацию о приложениях, услугах или интернет-сайтах, посещенных нашими пользователями во время подключения к нашему сервису. TunnelBear НЕ хранит подобную информацию». tunnelbear.com/privacy-policy/

howtogeek.com/215730/how-to-connect-to-a-vpn-from-your-iphone-or-ipad/

howtogeek.com/135036/how-to-connect-to-a-vpn-on-android/? PageSpeed=noscript

cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881

telegraph.co.uk/news/worldnews/northamerica Petraeus-ordered-lover-Paula-Broadwell-to-stop-emailing-Jill-Kelley.html

nytimes.com/2012/11/12/us/us-officials-say-petraeuss-affair-known-in-summer.html

howtogeek.com/192173/how-and-why-to-change-your-mac-address-on-windows-linux-and-mac/? PageSpeed=noscript

Глава 9

wired.com/2012/12/ff-john-mcafees-last-stand/

defensetech.org/2015/06/03/us-air-force-targets-and-destroys-isis-hq-building-using-social-media/

bbc.com/future/story/20150206-biggest-myth-about-phone-privacy

dailymail.co.uk/news/article-3222298/Is-El-Chapo-hiding-Costa-Rica-Net-closes-world-s-wanted-drug-lord-hapless-son-forgets-switch-location-data-Twitter-picture.html

threatpost.com/how-facebook-and-facial-recognition-are-creating-minority-report-style-privacy-meltdown-080511/75514

forbes.com/sites/kashmirhill/2011/08/01/how-face-recognition-can-be-used-to-get-your-social-security-number/2/

searchengineland.com/with-mobile-face-recognition-google-crosses-the-creepy-line-70978

Robert Vamosi, When Gadgets Betray Us: The Dark Side of Our Infatuation with New Technologies (New York: Basic Books, 2011)

forbes.com/sites/kashmirhill/2011/08/01/how-face-recognition-can-be-used-to-get-your-social-security-number/

techcrunch.com/2015/07/13/yes-google-photos-can-still-syncyour-photos-after-you-delete-the-app/

facebook.com/legal/terms

consumerreports.org/cro/news/2014/03/how-to-beat-facebook-s-biggest-privacy-risk/index.htm

forbes.com/sites/amitchowdhry/2015/05/28/facebook-security-checkup/

consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/ index.htm

cnet.com/news/facebook-will-the-real-kevin-mitnick-please-stand-up/

eff.org/files/filenode/social_network/training_course.pdf

bits.blogs.nytimes.com/2015/03/17/pearson-under-fire-for-monitoring-students-twitter-posts/

washingtonpost.com/blogs/answer-sheet/wp/2015/03/14/pearson-monitoring-social-media-for-security-breaches-during-parcc-testing/

csmonitor.com/World/Passcode/Passcode-Voices/2015/0513/Is-student-privacy-erased-as-classrooms-turn-digital

motherboard.vice.com/en_us/article/78857e/so-were-sharing-our-social-security-numbers-on-social-media-now

pix11.com/2013/03/14/snapchat-sexting-scandal-at-nj-high-school-could-result-in-child-porn-charges/

bbc.co.uk/news/uk-34136388

ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were

informationweek.com/software/social/5-ways-snapchat-violated-your-privacy-security/d/d-id/1251175

fusion.net/story/192877/teens-face-criminal-charges-for-taking-keeping-naked-photos-of-themselves/

bbc.com/future/story/20150206-biggest-myth-about-phone-privacy

fusion.net/story/141446/a-little-known-yelp-setting-tells-busi-nesses-your-gender-age-and-hometown/?utm_source=rss&utm_ medium=feed&utm_campaign=/author/kashmir-hill/feed/

На устройствах iPhone/iPad коснитесь значка **Настройки** (Settings) и выберите пункт **Конфиденциальность —> Службы геолокации** (Privacy —> Location Services). В этом разделе вы найдете список всех приложений, отслеживающих ваше местонахождение. Например, можно отключить геолокацию только в приложении Facebook Messenger. Прокрутите список до строчки Facebook Messenger и задайте настройке геолокации приложения значение Никогда (Never). На устройствах с Android откройте приложение Facebook Messenger, щелкните по значку настроек (в форме шестеренки) в верхнем правом углу, прокрутите до строчки **Новые сообщения по умолчанию включают данные о вашем местонахождении** (New messages include your location by default) и снимите флажок. На устройствах с Android, как правило, необходимо отключать геолокацию для каждого приложения по отдельности (если есть такая возможность). Отключить геолокацию для всего устройства нельзя.

blog.lookout.com/blog/2016/08/25/trident-pegasus/

Глава 10

В новейших версиях iOS можно отключить GPS следующим образом: smallbusiness.chron.com/disable-gps-tracking-iphone-30007.html

gigaom.com/2013/07/08/your-metadata-can-show-snoops-a-whole-lot-just-look-at-mine/

zeit.de/datenschutz/malte-spitz-data-retention

washingtonpost.com/local/public-safety/federal-appeals-court-that-includes-va-md-allows-warrantless-tracking-of-historical-cell-site-records/2016/05/31/353950d2-2755-11e6-a3c40724e8e24f3f_story.html

fusion.net/story/177721/phone-location-tracking-google-feds/?utm_source=rss&utm_medium=feed&utm_campaign=/author/kashmir-hill/feed/

forbes.com/sites/andyrobertson/2015/05/19/strava-flyby/?ss=future-tech

fusion.net/story/119745/in-the-future-your-insurance-company-will-know-when-youre-having-sex/?utm_source=rss&utm_medium=feed&utm_campaign=/author/kashmir-hill/feed/

thenextweb.com/insider/2011/07/04/details-of-fitbit-users-sex-lives-removed-from-search-engine-results/

fusion.net/story/119745/in-the-future-your-insurance-company-will-know-when-youre-having-sex/?utm_source=rss&utm_ medium=feed&utm_campaign=/author/kashmir-hill/feed/

engadget.com/2015/06/28/fitbit-data-used-by-police/

abc27.com/2015/06/19/police-womans-fitness-watch-disproved-rape-report/

theguardian.com/technology/2014/nov/18/court-accepts-data-fit-bit-health-tracker

smithsonianmag.com/innovation/invention-snapshot-changed-way-we-viewed-world-180952435/?all&no-ist

books.google.com/books?id=SlMEAAAAMBAJ&pg=PA158&lpg=PA158&dq=%22The+kodak+has+added+a+new+terror+to+the+picnic%22&source=bl&ots=FLtKbYGv6Y&sig=YzE2BisTYejb1pT3

ALv2-S3Cg&ved=0CCAQ6AEwAA#v=onepage&q=%22The%20koda&f=false

smithsonianmag.com/innovation/invention-snapshot-changed-way-we-viewed-world-180952435/?no-ist=&page=2

faa.gov/uas/media/Part_107_Summary.pdf

faa.gov/uas/where_to_fly/b4ufly/

slate.com/articles/technology/future_tense/2015/06/facial_recognition_privacy_talks_why_i_walked_out.html

extremetech.com/mobile/208815-how-facial-recognition-will-change-shopping-in-stores

retail-week.com/innovation/seven-in-ten-uk-shoppers-find-facial-recognition-technology-creepy/5077039.article

ilga.gov/legislation/ilcs/ilcs3.asp? ActID=3004&ChapterID=57

arstechnica.com/business/2015/06/retailers-want-to-be-able-to-scan-your-face-without-your-permission/

fusion.net/story/154199/facial-recognition-no-rules/?utm_ source=rss&utm_medium=feed&utm_campaign=/author/kashmir-hill/feed/

youtube.com/watch?v=NEsmw7jpODc

motherboard.vice.com/read/glasses-that-confuse-facial-recognition-systems-are-coming-to-japan

Глава 11

wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Совершенно бессмысленно. Если что-то запрещено, не значит, что этого не случится. Опасность ситуации заключается в том, что взломанная машина может навредить остальным участникам движения. Уязвимость нулевого дня для автомобилей, как вам такое?

keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/

buzzfeed.com/johanabhuiyan/uber-is-investigating-its-top-new-york-executive-for-privacy

theregister.co.uk/2015/06/22/epic_uber_ftc/

nypost.com/2014/11/20/uber-reportedly-tracking-riders-without-permission/

uber.com/legal/usa/privacy

fortune.com/2015/06/23/uber-privacy-epic-ftc/

bbc.com/future/story/20150206-biggest-myth-about-phone-privacy

tech.vijayp.ca/of-taxis-and-rainbows-f6bc289679a1

arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/

Можно купить и пополнять транспортную карту за наличные, но это не всегда удобно, а в некоторых случаях требует дополнительной траты времени на то, чтобы предварительно снять деньги с банковской карты или счета.

wsj.com/articles/SB10000872396390443995604578004723603576296

aclu.org/blog/free-future/internal-documents-show-fbi-was-wrestling-license-plate-scanner-privacy-issues

wired.com/2015/05/even-fbi-privacy-concerns-license-plate-readers/

В пяти случаях владельцами камер были: офис шерифа Прихода Сент-Тэмэни, офис шерифа Прихода Джефферсон и полицейское управление города Кеннер в Луизиане, департамент полиции города Хайалиа во Флориде и управление общественной безопасности Университета Южной Калифорнии.

forbes.com/sites/robertvamosi/2015/05/04/dont-sell-that-connected-car-or-home-just-yet/

washingtonpost.com/blogs/the-switch/wp/2015/06/24/tesla-says-its-drivers-have-traveled-a-billion-miles-and-tesla-knows-how-many-miles-youve-driven/

dhanjani.com/blog/2014/03/curosry-evaluation-of-the-tesla-model-s-we-cant-protect-our-cars-like-we-protect-our-workstations. html

teslamotors.com/blog/most-peculiar-test-drive

forbes.com/sites/kashmirhill/2013/02/19/the-big-privacy-take-away-from-tesla-vs-the-new-york-times/

wired.com/2015/07/gadget-hacks-gm-cars-locate-unlock-start/

spectrum.ieee.org/cars-that-think/transportation/advanced-cars/ researchers-prove-connected-cars-can-be-tracked

wired.com/2015/10/cars-that-talk-to-each-other-are-much-easier-to-spy-on/

grahamcluley.com/2013/07/volkswagen-security-flaws/

grahamcluley.com/2015/07/land-rover-cars-bug/

wired.com/2015/07/hackers-remotely-kill-jeep-highway/

forbes.com/sites/robertvamosi/2015/03/24/securing-connected-cars-one-chip-at-a-time/

nytimes.com/2016/07/30/business/tesla-faults-teslas-brakes-but-not-autopilot-in-fatal-crash.html

Глава 12

amazon.com/review/R3IMEYJFO6YWHD

blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your-Home.pdf

venturebeat.com/2014/08/10/hello-dave-i-control-your-thermo-stat-googles-nest-gets-hacked/

forbes.com/sites/kashmirhill/2014/07/16/nest-hack-privacy-tool/

venturebeat.com/2014/08/10/hello-dave-i-control-your-thermostat-googles-nest-gets-hacked/

networkworld.com/article/2909212/security0/schneier-on-really-bad-iot-security-it-s-going-to-come-crashing-down.html

forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/

wired.com/2009/11/baby-monitor/

bbc.com/news/technology-31523497

mashable.com/2012/05/29/sensory-galaxy-s-iii/

forbes.com/sites/marcwebertobias/2014/01/26/heres-how-easy-it-is-for-google-chrome-to-eavesdrop-on-your-pc-microphone/

theguardian.com/technology/2015/jun/23/google-eavesdropping-tool-installed-computers-without-permission

Вероятно, для этого проще всего открыть приложение Amazon Echo и выбрать меню Settings — > History — > Tap Individual Recording — > Delete.

Зайдите в свою учетную запись на сайте amazon.com, в разделе **Account Settings** выберите пункт **Your Devices** —> **Amazon Echo** —> **Delete**.

theregister.co.uk/2015/08/24/smart_fridge_security_fubar/

Глава 13

wsj.com/articles/SB10001424052702303672404579151440488919138

theweek.com/articles/564263/rise-workplace-spying

olin.wustl.edu/docs/Faculty/Pierce_Cleaning_House.pdf

harpers.org/archive/2015/03/the-spy-who-fired-me/

room362.com/post/2016/snagging-creds-from-locked-machines/

Как правило, метаданные документа скрыты. Чтобы их увидеть, выберите меню File (Файл) > Info (Сведения), а затем просмотрите свойства в правой части окна.

При использовании инструмента «Инспектор документов» сначала сделайте копию своего документа, поскольку внесенные изменения нельзя будет отменить. В созданной копии вашего документа щелкните по вкладке File (Файл) > **Info** (Сведения). В разделе **Prepare for Sharing** (Подготовить к общему доступу) щелкните по кнопке **Check for Issues** (Поиск проблем) и в открывшемся меню выберите пункт **Inspect Document** (Инспектор документов). В открывшемся диалоговом окне установите флажки возле содержимого, которое требуется проверить. Щелкните по кнопке **Inspect** (Проверить). Просмотрите результаты проверки в диалоговом окне **Document Inspector** (Инспектор документов). Щелкните по кнопке **Remove All** (Удалить все) рядом с результатами проверки, чтобы удалить из документа все требуемое содержимое.

infosecurity-magazine.com/news/printer-related-security-breaches-affect-63-of/

wired.com/2014/08/gyroscope-listening-hack/

ossmann.blogspot.com/2013/01/funtenna.html

cs229.stanford.edu/proj2013/Chavez-ReconstructingNon-IntrusivelyCollectedKeystrokeDataUsingCellphoneSensors.pdf

ru.scribd.com/document/172841592/Traynor-ccs11-Decoding-Vibrations-From-Nearby-Keyboards

samy.pl/keysweeper/

wired.com/2015/10/stingray-government-spy-tools-can-record-calls-new-documents-confirm/

phys.org/news/2013-07-femtocell-hackers-isec-smartphone-content.html

arstechnica.com/information-technology/2015/04/this-machine-catches-stingrays-pwnie-express-demos-cellular-threat-detector/

guardian.co.uk/world/2013/jul/11/microsoft-nsa-collaboration-user-data

computerworld.com/article/2474090/data-privacy/new-snowden-revelation-shows-skype-may-be-privacy-s-biggest-enemy.html

community.rapid7.com/community/metasploit/blog/2012/01/23/ video-conferencing-and-self-selecting-targets

docs.polycom.com/global/documents/solutions/industry_solutions/government/max_security/uc-deployment-for-maximum-security.pdf

community.rapid7.com/community/metasploit/blog/2012/01/23/video-conferencing-and-self-selecting-targets

Например, boxcryptor.com/ru/

Глава 14

То, что этот обыск и арест производятся на границе, не имеет особого значения. Суды США пока еще не обязали обыскиваемого человека выдавать свой пароль. Тем не менее суд постановил, что этот человек может быть принужден к прохождению процедуры аутентификации на своем iPhone с помощью функции Touch ID (аутентификация по отпечатку пальца). Чтобы не рисковать, всякий раз при прохождении таможенного досмотра в любой стране перезагружайте свой телефон или любое другое устройство Apple с функцией Touch ID и не вводите свой код доступа. Пока вы не введете код доступа, функция Touch ID не сработает.

computerweekly.com/Articles/2008/03/13/229840/us-department-of-homeland-security-holds-biggest-ever-cybersecurity.htm

В операционной системе iOS8 или более поздней версии вы можете сбросить все сертификаты сопряжения, коснувшись значка **Настройки** (Settings), выбрав пункт **Основные** —> **Сброс** (General —> Reset), а затем коснувшись пункта **Сбросить геонастройки** (Reset Location & Privacy) или **Сбросить настройки сети** (Reset Network Settings). Исследователь Джонатан Здзиарски написал несколько постов в своем блоге, посвященных этой теме. Эти инструкции выходят за пределы данной книги, однако если вас серьезно интересует этот вопрос, посетите блог zdziarski. com/blog/?p=2589

engadget.com/2014/10/31/court-rules-touch-id-is-not-protected-by-the-fifth-amendment-bu/

cbc.ca/news/canada/nova-scotia/quebec-resident-alain-philippon-to-fight-charge-for-not-giving-up-phone-password-at-airport-1.2982236

ghacks.net/2013/02/07/forensic-tool-to-decrypt-truecrypt-bitlocker-and-pgp-contains-and-disks-released/

symantec.com/content/en/us/enterprise/white_papers/b-pgp_how_wholedisk_encryption_works_WP_21158817.en-us.pdf

kanguru.com/storage-accessories/kanguru-ss3.shtml

schneier.com/blog/archives/2007/11/the_strange_sto.html

theintercept.com/2015/04/27/encrypting-laptop-like-mean/

securityweek.com/researcher-demonstrates-simple-bitlocker-by-pass

fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

nytimes.com/library/tech/00/01/cyber/cyberlaw/28law.html

partners.nytimes.com/library/tech/00/01/cyber/cyberlaw/28law.html

wired.com/2015/10/cops-dont-need-encryption-backdoor-to-hack-iphones/

theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html

blog.gdatasoftware.com/blog/article/hotel-safes-are-they-really-safe.html

snopes.com/crime/warnings/hotelkey.asp

themarysue.com/hotel-key-myth/

shaun.net/posts/whats-contained-in-a-boarding-pass-barcode

Очевидно, авиакомпания United Airlines является одной из немногих, предоставляющих только часть номера часто летающего пассажира. Большинство авиакомпаний зашифровывают в штрих-коде этот номер целиком. wired.com/2014/11/darkhotel-malware/

bitlaunder.com/launder-bitcoin

Глава 15

wired.com/2015/05/silk-road-creator-ross-ulbricht-sentenced-life-prison/

nytimes.com/2015/12/27/business/dealbook/the-unsung-tax-agent-who-put-a-face-on-the-silk-road.html?_r=0

wired.com/2015/07/online-anonymity-box-puts-mile-away-ip-address/

samy.pl/proxygambit/

Глава 16

Это не все. Несмотря на то что ФБР удалось определить многоквартирный дом, в котором я жил, они не знали, где конкретно я находился. Все изменилось однажды вечером, когда я вышел на улицу. Подробности этой истории можно найти в моей книге «Призрак в сети» (Ghost in the Wires).

Такие сайты, как Weather Underground, включают географические координаты посетителя в URL-адрес.

Например, bitrefill.com.

nakedsecurity.sophos.com/2015/07/30/websites-can-track-us-by-the-way-we-type-heres-how-to-stop-it/

* * *

Примечания

1

DEF CON — старейший и один из крупнейших слетов хакеров. — *Здесь и далее прим. ред*.

2

TED — американский частный некоммерческий фонд, известный своими ежегодными конференциями, главная цель которых — распространять уникальные идеи. Некоторые выступления доступны в Интернете.

3

«Патриотический акт» — федеральный закон, принятый в США в октябре 2001 года, который дает правительству и полиции широкие полномочия по надзору за гражданами. Принят после террористического акта 11 сентября 2001 года.

4

Аналог СНИЛС/ИНН в РФ.

5

«Тутти-фрутти» — это темно-розовый цвет.

6

В России не получили распространения. Как правило, стоят дороже iPad.

7

Автор говорит о телефонах с предоплатной системой расчетов. В России все SIM-карты продаются по паспорту, поэтому данный метод неактуален.

8

Скрипт-кидди — от англ. *Script kiddie,* что можно примерно перевести как «сопляк со скриптами» — принятое у хакеров название для неопытного взломщика, пользующегося готовыми скриптами и программами, не понимая механизма их действия и не будучи в состоянии написать что-то свое.

9

В англосаксонской системе права, принятой в США, принято разделять нарушения закона на тяжкие преступления (felony) и проступки (misdemeanor).

10

Мессенджер Telegram запрещен на территории РФ.

11

Там находится столица США, город Вашингтон.

12

Она же киноа, южноамериканская зеровая культура.

13

Американский бейсболист.

14

В октябре 2018 г. компания Google объявила о ее закрытии.

15

В некоторых операционных системах, например Windows и Windows Mobile, наоборот, значками помечаются открытые беспроводные сети (значком щита с восклицательным знаком).

16

Террористическая организация, запрещенная в РФ.

17

В настоящее время их количество увеличилось до 280 символов.

18

Люди, родившиеся после 1996 года.

19

Отсылка к телесериалу «Рыцарь дорог», в котором участвует машина с искусственным интеллектом под названием КИТТ (англ. K.I.T.T. — Knight Industries Two Thousand, Рыцарь дорог две тысячи).

20

Система телематики для автомобилей General Motors, предлагающая водителям широкий спектр информационных услуг.

21

Женское имя Элис (Alice) начинается с первой буквы алфавита и употребляется в смысле «любой человек», «имярек». Это соответствует русскому «Иванов, Петров, Сидоров».

22

Компьютер из известного фильма «Космическая одиссея 2001» режиссера Стэнли Кубрика.

23

Всеволновой радиоприемник.

24

Документ, содержащий его кредитный рейтинг.

25

Последняя рабочая версия TrueCrypt.

26

Термин, означающий такое поведение, при котором, совершив действие или отдав распоряжение, можно затем отрицать это без существенного риска быть уличенным во лжи.