Глава 2

Наши цифровые ценности

В этой главе мы рассмотрим виды цифровых активов, которые уже есть (или скоро будут) почти у всех, и увидим, что они обладают реальной ценностью, а потому их надо беречь также, как и привычные вещи — деньги, имущество и другое.

Многие считают себя «цифровыми бедняками» — мол, красть у нас нечего, потому и замки не нужны. Когда человек не осознает, что у него есть что-то ценное, любые меры предосторожности кажутся ему избыточными.

Когда человек не осознает, что у него есть что-то ценное, любые меры предосторожности кажутся ему избыточными.

Скорее всего, в ответ на ваши советы он покрутит пальцем у виска и назовет вас параноиком. В реальной жизни ведь никто не будет ставить мегазащищенную железную дверь, если в доме шаром покати — вот когда привалит богатство, тогда и подумаем об этом.

Такую точку зрения можно признать вполне рациональной, поскольку стоимость и сложность системы защиты должна быть адекватна ценности того, что мы пытаемся с ее помощью защитить. Однако в том, что касается цифровых ценностей, наш житейский опыт не всегда выступает хорошим советчиком: слишком внезапно произошли изменения, и у нас еще не выработались привычки, позволяющие действовать правильно «на автомате», не задумываясь. Поэтому даже многие взрослые, опытные во всех отношениях люди часто попадают впросак, когда сталкиваются с киберпреступниками или сами случайно уничтожают что-то для себя ценное.

Прежде всего, давайте проведем инвентаризацию наших цифровых активов, чтобы понять их истинную ценность, а уже потом подумаем, как их защитить от возможных посягательств преступников и от собственной глупости.

Итак, что у нас сегодня в «цифре»? Да почти все! Информационные технологии просочились всюду, и, помимо того, что дали нам кучу

новых возможностей, везде добавили новых рисков, которые теперь надо учитывать.

Условно наши цифровые богатства можно разделить на три категории:

- «**Измененные цифрой**» — то, что существовало и раньше, но под воздействием новых технологий претерпело значительные трансформации. Например, деньги. В этой сфере безопасность наших данных и ресурсов во многом зависит от действий других людей, на которых мы повлиять не можем. А между тем сами институты, поддерживающие эти ценности, тоже не до конца понимают масштабы новых угроз.

- «**Рожденные в цифре**» — это различные цифровые объекты, которые мы создаем сами, покупаем или которыми пользуемся. Все они, по сути, представляют собой лишь информацию, записанную в компьютерных системах, а у нас могут быть различные права на них. Например, виртуальный танк или персональная страница в соцсети. Их сохранность во многом зависит от того, насколько хорошо мы соблюдаем правила безопасности, и, конечно же, от квалификации разработчика.

- «**Кибервещи**» — сейчас каждая кофеварка норовит выйти в интернет. То есть обычные физические вещи становятся цифровыми, а значит, об их безопасности тоже надо позаботиться — это относительно новое явление, с которым еще предстоит разобраться.

Теперь давайте перечислим, что́ это могут быть за «богатства» (хотя, почему в кавычках?):

- **Деньги**. Кроме наличных в кошельке, они все электронные;
- **Бонусы**. «Как бы деньги» — мили, баллы лояльности и прочее;
- **Персональные данные, включая медицинские**. Пока это просто информация — до тех пор, пока кто-то не решит украсть и продать вашу цифровую личность;
- **Аккаунты в соцсетях, страницы и каналы**. Иногда это очень дорогой актив;
- **Цифровые авторские права на сайты, блоги, фото, видео и другой контент**;
- **Тайна частной жизни.** Когда вокруг камеры и микрофоны, это становится не просто богатством, а роскошью;
- **Репутация.** Все, что написано о вас, и все, что вы написали сами, сохраняется в интернете навечно. А ведь репутация — один из самых дорогих активов;
- **Переписка**, деловая и личная, в электронной почте и мессенджерах;
- **Цифровые коллекции.** Музыка, кино, файлы, фотографии (разумеется, без пиратских копий);
- **Виртуальные вещи.** Пока в играх, дальше будет больше;
- **Контакты и заметки**. Ведь никто уже не держит записных книжек, не так ли?;

- **Домены (сайты)**. В наше время уже бывает, что даже имя ребенку выбирают такое, чтобы домен был свободен;

- **Цифровые ресурсы.** Домашний wi-fi, место в облачном хранилище, виртуальные машины и тому подобное;

- **Цифровая техника.** Телефон, компьютер и прочая умная электроника;

- **Автомобиль**, который все больше превращается в компьютер на колесах со всеми вытекающими отсюда рисками;

- **Умный дом.** Эта тема только набирает популярность и пока не слишком волнует киберпреступников, но угрозы будут расти.

Ого, сколько, оказывается, всего у нас есть ценного! Естественно, найдутся люди, которые могут захотеть это украсть или уничтожить.

Теперь давайте посмотрим на наше «цифровое богатство» более подробно.

Деньги в эпоху цифры

Кроме наличных, которые лежат у вас в кармане, все остальные ваши деньги существуют в цифровом виде. Зарплата на карточке, депозит в банке, баланс на счете мобильного телефона, небольшой резерв в электронном кошельке Киви или «Яндекс» — это ведь не более чем цифры в какой-то базе данных. Но это такие же на-

стоящие деньги, как и наличные. И их точно также можно потерять. Или стать жертвой грабителей.

Ясно, что финансовые системы — одни из наиболее защищенных, но они же являются и самым лакомым куском для киберпреступников.

Это есть в главе про социнженеров. Как же они это делают? В основном — благодаря невнимательности граждан. Чаще всего жулики используют поддельные сайты (фишинг) и методы социальной инженерии, когда человек фактически сам отдает им деньги. Особенно активизировались в последнее время телефонные мошенники, вооруженные вашими персональными данными. Обычно они представляются службой безопасности банка и в разговоре выманивают у вас недостающую информацию, чтобы совершить перевод с вашего счета себе.

> *Центральный банк РФ (ЦБ РФ) подчеркивает, что социальная инженерия — это главная угроза информационной безопасности. «Более 97% хищений со счетов физических лиц и 39% хищений со счетов юридических лиц были совершены с использованием приемов социальной инженерии», — рассказал на форуме «Финополис» первый замглавы департамента информационной безопасности ЦБ РФ Артем Сычев*[1].

Увы, надежного метода защиты от социальной инженерии не существует. На удочку таких жуликов попадаются даже специалисты по информационной безопасности — потому что все мы живые люди и у нас есть эмоции, которые могут отключить наше критическое мышление.

---

1 «Вам звонят из банка»: как воруют наши деньги. // Газета.ru, 10 октября 2019.

Тем не менее, стоит еще раз повторить:

- Сотрудники банка никогда не спрашивают у клиентов проверочный код карты[1], ПИН-код и SMS-пароли. Но будьте осторожны: преступники тоже знают, что вы это знаете, и научились изображать переключение на якобы информационную систему банка, куда просят ввести ваш код;

- Железное правило: получив звонок о подозрительной операции по вашему счету, положите трубку и сами перезвоните в банк. Помните, что у вас нет никакой возможности проверить подлинность входящего звонка. Преступники умеют подменять свой номер на номер банка;

- Будьте крайне внимательны с SMS. Мошенники легко имитируют названия банков в качестве отправителей, но их сообщение упадет в новую переписку, и это должно вас насторожить. А если SMS, полученное как будто бы от банка, предлагает перейти по какой-то ссылке, то это почти наверняка жулики. Не поленитесь перезвонить в банк и узнать, действительно ли вам отправляли такое сообщение и зачем.

Главное — не поддаваться во время звонка панике, когда вам сказали, что ваши деньги вот-вот украдут, или, наоборот, эйфории, если вам позвонили, чтобы поздравить с небывалым выигрышем. Спокойно проанализируйте ситуацию и возьмите инициативу в свои руки, не поддавайтесь на разводку мошенников — хотя это проще

---

1 *У каждой платежной системы свое наименование секретного кода безопасности: у VISA — это код CVV2 (Card Verification Value 2); у MasterCard — CVC2 (Card Verification Code 2); у American Express — CID (Card Identification); у НПСК МИР — CVP2 (Card Verification Parameter 2).*

сказать, чем сделать. И на всякий случай будьте вежливы: иногда звонят настоящие сотрудники банков, которые действительно заботятся о сохранности ваших средств.

Безопасность ваших цифровых финансов далеко не всегда зависит от вас. Преступники, как и во времена Бонни и Клайда, все также любят грабить банки, а не отдельных клиентов. Только вместо шумных нападений со стрельбой и погонями теперь они действуют тихо: максимум, что можно услышать, это клацанье клавиш компьютера. И, надо сказать, действуют они гораздо эффективнее, чем грабители прошлого века.

> *В 2015 году прогремело известие о масштабном ограблении банков по всему миру. Более 30 компаний понесли ущерб на общую сумму порядка 1 миллиарда долларов. Это была умело проведенная хакерская атака. Мошенники заразили вирусами банки Украины, России, Европы, Китая, Юго-Восточной Азии, Ближнего Востока и Африки. И в течение двух лет незаметно крали у них деньги.*
>
> *Схема внедрения вируса была проста: на электронную почту работнику банка приходило письмо, содержащее вложение с вредоносной программой. После проникновения вируса на компьютер мошенники начинали отслеживать принципы работы каждой конкретной банковской системы. Все действия, которые позже производили хакеры, — перевод денежных средств, управление банкоматами — совершались якобы от имени банковских служащих. А до этого кибермошенники серьезно изучали схему работы сотрудников, в том числе через камеры*[1].

---

1 *Самое крупное киберограбление банков в истории на 1 миллиард долларов. // Яндекс.Дзен, 6 декабря 2018.*

Не наше дело указывать банкам, что и как им следует делать для повышения безопасности наших средств. Прежде всего, нужно уделить внимание безопасности собственных цифровых финансов, — тем более, что оборот наличных в мире неуклонно сокращается, а доля электронных платежей растет. Сейчас стало модно, особенно среди молодежи, не иметь при себе наличных и везде расплачиваться карточкой, а еще лучше — телефоном. Удобно? Несомненно. Рискованно? Не без этого. Но при соблюдении простых правил эти риски можно снизить до приемлемого уровня.

Бонусы. «Как бы деньги»

Кроме банковских карт у вас в кошельке наверняка есть еще куча разнообразного пластика — бонусные и скидочные карты, карты лояльности от авиакомпаний и тому подобное. Некоторые из них не жалко и выбросить, другие же имеют высокую ценность.

Но и этот пластик чаще всего есть всего лишь физическое воплощение неких цифр. Если вы потеряете саму карточку — это не страшно: попросите новую. А вот если кто-то получит доступ к вашему аккаунту, то он, скорее всего, найдет способ, как употребить ваши бонусные баллы. Формально, с точки зрения Центрального Банка, все эти баллы и бонусы деньгами не являются, но с практической точки зрения они равнозначны настоящим деньгам. Будет обидно, если вы целый год, летая по командировкам, копили мили, чтобы взять бесплатный билет и отправиться в отпуск, а кто-то их возьмет и украдет. Ваш кошелек испытает такую же боль, как если бы из него внезапно вытащили несколько крупных купюр.

Такой случай произошел в 2015 году, когда хакерской атаке подверглись аккаунты участников программы «Аэрофлот Бонус». Злоумышленники пытались украсть у клиентов авиакомпании бонусные мили, и, чтобы остановить атаку, «Аэрофлоту» пришлось временно заблокировать у ряда пользователей мили на списание. Получить доступ к аккаунтам клиентов хакеры могли через почтовые ящики. В связи с этим «Аэрофлот» рекомендовал пользователям устанавливать разные логины и пароли на почту и личный кабинет в программе «Аэрофлот Бонус»[1].

Но не всем клиентам «Аэрофлота» так повезло. У жительницы Хабаровска накопленные за несколько лет заветные мили для перелетов со скидками таинственно исчезли из личного кабинета. Вот что она рассказала (стиль, орфография и пунктуация сохранены):

> *«В августе 2015 года я обнаружила значительное уменьшение накопленных мною за четыре года миль, а именно исчезло 97,5 тысячи. Зайдя в личный кабинет, увидела то, что три человека с конкретными Ф.И.О. и номерами документов в разные дни августа совершили перелет бизнес-классом по направлению Москва-Адлер. При этом оплатили они их милями с моего счета. ... В ответ на мои неоднократные устные и письменные заявления в компанию «Аэрофлот» я получала ответы будто моим вопросом занимаются, а такая ситуация впервые случилась и так далее»[2].*

---

1 *Хакеры попытались украсть бонусные мили у клиентов «Аэрофлота» // РБК, 12 августа 2015.*

2 *Кража по-русски: Участие в программе «Аэрофлот Бонус» хабаровчанка запомнит надолго // AmurMedia.ru, 18 ноября 2015*

Авиакомпания выразила сожаление, но помочь клиенту не смогла, ссылаясь на то, что услуга по перевозке была оказана в полном объеме, и посоветовала обратиться в правоохранительные органы.

Аналогичный случай был и в 2018 году. Клиент получил сообщение, что кто-то зашел в его личный кабинет и сменил телефон для SMS-информирования. Злоумышленник также поменял пароль, и теперь законный пользователь не мог получать уведомления о списании миль и контролировать свой счет. Он сразу же обратился в авиакомпанию, и после некоторых волнений ситуация все же разрешилась благополучно (стиль, орфография и пунктуация сохранены):

> *«По Вашему обращению в контакт-центр авиакомпании оператором, а затем службой экономической безопасности были предприняты необходимые действия по отмене несанкционированно оформленной перевозки. Мили возвращены на Ваш счет. Соответствующими подразделениями авиакомпании проводится работа по расследованию и упреждению подобных случаев. Выражаем надежду, что меры по защите счетов участников, предпринимаемые как со стороны авиакомпании, так с Вашей стороны, как владельца Личного кабинета, позволят не допустить подобных ситуаций в дальнейшем»*[1].

Подобные хищения — дело рук не каких-то хакеров-одиночек, а результат работы организованного киберпреступного сообщества в составе примерно двадцати человек. Мошенники получали доступ к аккаунтам участников программы «Аэрофлот Бонус», а потом продавали мили желающим приобрести билеты подешевле. Это слож-

1 *Кражи в Аэрофлоте // ЖивойЖурнал, блогер «nemihail», 13 сентября 2018.*

ное уголовное дело вела следователь управления на транспорте МВД по ЦФО Евгения Шишкина, которая была убита в ноябре 2018 года. Как писала газета «Коммерсантъ», начатое Шишкиной расследование, по данным близкого к нему источника «Ъ», продвигалось с большим трудом. Участники, например, постоянно спорили, можно ли считать похищенными мили, строго говоря, не имеющие материальной ценности, и кто в таком случае является потерпевшим — обворованный фактически клиент или авиакомпания — юридический владелец миль. Споры, по данным того же источника, приводили и к конфликтам, вышедшим в итоге за стены следственного кабинета[1].

Преступников юридические тонкости не волнуют — считать ли мили и прочие бонусы настоящими деньгами или нет. Зато они четко видят возможность заработать на их краже и могут пойти на любые действия, чтобы сохранить свой нелегальный бизнес. История трагическая, но весьма показательная.

Персональные данные

1984 год, Лос-Анджелес. Из уже недалекого от нас 2029 года, где идет война людей с машинами, в прошлое заброшен робот Терминатор, который должен найти и убить Сару Коннор, мать будущего предводителя Сопротивления. Чтобы его остановить, следом прибывает сержант элитного подразделения Кайл Риз. И что они оба делают? Идут к ближайшей телефонной будке, где лежит справоч-

1 *Полицейский следователь не поверила в госзащиту // Газета «Коммерсантъ», 11 октября 2018.*

ник, в котором они находят ее телефон и домашний адрес. Дальше вы знаете.

Для современного зрителя это выглядит шокирующим. Неужели персональные данные всех граждан вот так спокойно лежат в каждой телефонной будке, и кто угодно может их прочитать? Сегодня это бы назвали крупной утечкой и обсуждали бы во всех новостях, а на виновника наложили бы крупный штраф. За подобную промашку Facebook* предстоит выложить кругленькую сумму в 5 миллиардов долларов[1] — и это на сегодня самое крупное взыскание с технологической компании. Ранее Google в подобной ситуации был оштрафован на 22,5 миллиона долларов.

> *По сравнению с США, в России штрафы пока выглядят символическими, даже с учетом их повышения в ноябре 2019 года. Теперь за допущенную утечку персональных данных юридическое лицо может заплатить от 1 до 6 миллионов рублей и от 6 до 18 миллионов рублей за повторное нарушение. Но для многих организаций и это может оказаться непосильным бременем.*

Что же заставило законодателей принять такие драконовские меры? Может быть, нашествие терминаторов, которого мы не заметили?

По правде говоря, какой-то одной причины нет. Скорее, это результат признания той огромной роли, которую стали играть в жизни общества информационные технологии, ведь благодаря им стала

---

* *Соцсеть признана экстремистской и запрещена на территории РФ.*

1 *FTC slaps Facebook* with record $5 billion fine, orders privacy oversight// CNBC, 24 июля 2019.*

возможной массовая обработка персональных данных, и принесла она с собой не только ощутимые удобства и блага, но и серьезные угрозы — поставленные на поток мошеннические схемы по краже денег с банковских карт, незаконные рекламные кампании и даже попытки влиять на исход выборов. То есть речь сегодня идет не о спасении какой-то конкретной Сары Коннор, а о противостоянии угрозам для общества в целом. С этих позиций жесткость властей выглядит объяснимой.

В России закон о защите персональных данных[1] был принят в 2006 году; с этого же момента развернулась и пиар-компания по просвещению пользователей, местами переходящая в форменную истерию. Судите сами: во всех статьях и роликах про защиту персональных данных нам рассказывают, как опасно оставлять в интернете домашний адрес и телефон и называть свое имя, однако при этом все мы спокойно сообщаем эти данные первому попавшемуся водителю такси или курьеру по доставке пиццы. Логично ли это?

Наши паспорта копируют и сканируют в десятках учреждений, нас фотографируют, снимают отпечатки наших пальцев, просят заполнить кучу бланков с разнообразными сведениями. Если посмотреть на вещи реально, то у человека, в общем-то, нет возможности управлять данными о себе. Безусловно, следует проявлять разумную осторожность и не оставлять лишней информации на совсем уж левых сайтах. Но не впадать же

1 *Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ, ст. 3 п.1: Персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).*

при этом в паранойю! Достаточно будет задать себе вопрос: для чего кому-то нужны ваши данные? Например, если вы не скажете адрес таксисту, он вас не довезет до дома. Однако совершенно необязательно рассказывать ему, с кем вы живете и сколько денег у вас на счете.

Вообще говоря, вся эта история с персональными данными больше касается бизнеса и государственных организаций, которые занимаются их обработкой. Кроме того, что на них лежит ответственность за утечки, они еще обязаны обеспечивать хранение и обработку наших данных в соответствии с требованиями регулятора, а это достигается путем покупки разнообразных сертифицированных средств; иначе нельзя.

> *Главная причина утечек данных российских пользователей — большое количество организаций, в которые они предоставляют информацию о себе, а также низкая зарплата сотрудников таких организаций*[1].

То есть мы, граждане, должны понимать, что изрядная доля шумихи вокруг защиты персональных данных связана с желанием поставщиков продать свои решения заказчикам, а отнюдь не с реальными угрозами. Понимая это, мы должны трезво взвесить свои риски при возможной утечке.

Первое, чем нас пугают профессиональные «защитники» наших данных — реклама. Дескать, узнав ваши контакты и предпочтения, вам все наперебой начнут делать предложения, от которых

---

1 *Результаты исследования, проведенного специалистами компании Ernst & Young, и опубликованного в TAdviser.*

вы не сможете отказаться. Но в чем же здесь риск? Если реклама окажется действительно полезной, это будет даже хорошо. Правда, некоторые рекламодатели бывают слишком назойливы и достают нас звонками по телефону, — так на это у нас есть черный список. Поэтому, положа руку на сердце, скажем: да, избыток рекламы — это некоторое неудобство, но никак не угроза безопасности.

Избыток рекламы — это некоторое неудобство, но никак не угроза безопасности.

Еще говорят, что, добыв копию вашего паспорта, кто-нибудь сможет оформить на него кредит. Да, такое случается, и полностью уберечься от этого риска невозможно, — даже если вы не будете пользоваться интернетом вовсе. Достаточно потерять паспорт или лишиться его вследствие кражи. Кроме того, копии паспортов требуются и хранятся в самых разных учреждениях, сотрудники которых не всегда могут быть в ладах с законом. Это обычное уголовное преступление, которое, к сожалению, не всегда легко расследуется. Зачастую человек узнает о висящем на нем долге, когда возникает серьезная просрочка, или даже на этапе исполнительного производства. В такой ситуации трудно дать какой-либо другой совет, кроме самого очевидного: обратиться в полицию.

Если вы потеряли паспорт или у вас возникли подозрения об утечке персональных данных, необходимо отправить запрос в Бюро кредитных историй — один раз в год это можно сделать бесплатно. Согласно закону «О кредитных историях», Бюро обязано выдать исчерпывающую информацию обо всех кредитах, взятых на ваше имя, и кредиторах.

Бывает, что мошенники оформляют на один добытый паспорт сразу несколько кредитов, поэтому лучше не ждать, когда к вам постучатся приставы. Считайте ежегодный запрос в БКИ одним из элементов цифровой гигиены, даже если вы не теряли паспорт.

А стоит ли паниковать, когда произошла утечка паспортных данных? Если вы подозреваете, что в руки мошенников мог попасть не сам паспорт, а только паспортные данные, то не стоит.

> *Александр Баранов, заведующий кафедрой информационной безопасности НИУ ВШЭ:*
>
> *«Наши паспортные данные растекаются направо и налево. Многие организации (например, гостиницы) требуют их предоставить, сканы документа остаются в салонах, где делают копии. Паспортные данные очень часто оказываются в открытом доступе, случается, что их продают или передают нечистые на руку банковские работники или сотрудники медицинских организаций. Если вы нашли свои паспортные данные в открытом доступе, можно написать жалобу в Роскомнадзор: этот орган занимается в России контролем за зашитой персональных данных и правильностью их передачи. Но это не повод, чтобы менять паспорт. Тем более что такое условие (утечка паспортных данных — прим. АиФ.ru) не является основанием для замены документа, в МВД вам откажут»*[1].

1 *В каких случаях стоит поменять паспорт? // Аргументы и Факты, 1 июля 2019.*

Медицинские данные

Среди персональных данных особо выделяют данные о состоянии здоровья — к их защите предъявляют повышенные требования. К таким данным относится информация о перенесенных заболеваниях, диагнозах, обследованиях, результаты анализов и даже сам факт обращения к врачу.

Почему люди так обеспокоены риском разглашения их истории болезни? В основном, из-за возможных социальных последствий. Увы, уровень образованности и толерантности в обществе не слишком высок, и поэтому некоторая информация, став публично известной, способна больно ударить по репутации и карьере. Например, факт обращения к психиатру может быть весьма негативно истолкован при приеме на работу — такому кандидату запросто откажут под каким-то надуманным предлогом. Но помилуйте, как человеку справляться, скажем, с депрессией? Лекарства в таких случаях может назначить только врач-психиатр. Есть, кроме того, «стыдные» болезни, которые никому не хочется афишировать.

Бывают ситуации, когда человек скрывает, что он действительно серьезно болен, хотя разглашение этой информации непосредственно его здоровью угрозы не несет. Некоторые же, наоборот, совершают «каминг-аут» и публично рассказывают о своем недуге. Иногда, кстати, это лучший способ пресечь слухи и даже помочь другим товарищам по несчастью, обратив таким образом внимание общества на проблему.

> *О том, что Фредди Меркьюри болен СПИДом, подозревали давно — он изменился внешне, перестал бывать на вечеринках, быстро утомлялся во время работы. Шила в мешке*

не утаишь, симптомы были слишком очевидны. Но публично Меркьюри заявил об этом только 23 ноября 1991 года, за день до смерти:

«Я заметил, что в последнее время все говорят о том, что я болен СПИДом. Это правда. У меня СПИД. Я долго скрывал эту информацию, чтобы мои друзья и родственники не беспокоились, но теперь в этом не вижу смысла. Я надеюсь, что многие из вас поймут, что со СПИДом нужно бороться. Только вместе мы сможем остановить эту страшную болезнь».

Он мог бы этого и не делать — посмертный диагноз легко можно было заменить на пневмонию — но Фредди все-таки принял решение сказать о своей болезни. В то время люди, больные СПИДом, подвергались стигматизации: их публично всячески порицали; не то чтобы излечивающих препаратов, но даже средств поддерживающей терапии еще не было. Сейчас мы понимаем, что ВИЧ может инфицироваться абсолютно любой человек, но в те годы эта была «болезнь геев».

На этом фоне поступок Фредди был не просто смелым: он сыграл важную роль в осведомленности о СПИДе и заставил миллионы людей задуматься об этом. Музыканты Queen приняли решение направить все деньги от переиздания самой знаменитой своей песни «Богемская рапсодия» на борьбу со СПИДом.

Пожалуй, едва ли кто-то будет озабочен тем, чтобы скрыть, что он переболел гриппом или повредил ногу, катаясь на горных лыжах. Но закон един: все это — персональные данные особой категории, которые должны охраняться. С другой стороны, строгость закона часто становится препятствием для развития медицинских

сервисов, потому что трудно создать даже обезличенные базы медицинских данных, не нарушив при этом требований закона 152-ФЗ о персональных данных.

Возможно, страхи насчет утечек медицинских данных изрядно преувеличены. Интуитивно люди это, пожалуй, чувствуют — недаром же в поезде часто рассказывают случайным попутчикам про все свои болезни. Но нужно признать, что существует риск, связанный с рекламой или попытками мошенничества: узнав ваши медицинские данные, некто может попытаться продать вам лекарственные препараты или медицинские услуги, в том числе и сомнительного качества. Больной человек не всегда поступает разумно и может попасться на удочку мошенников.

Больной человек не всегда поступает разумно и может попасться на удочку мошенников.

Также нужно помнить и о случаях, когда медработники «сливают» данные об умерших в ритуальные агентства, вследствие чего их родственники подвергаются агрессивной коммерческой атаке.

Аккаунты в социальных сетях

Миллиарды людей имеют аккаунты в соцсетях. С одной стороны, это окно в мир, возможность общаться и получать информацию. Взрослых, по понятным причинам, беспокоит наличие в сетях нежелательного контента, от которого они пытаются оградить детей, — это тема отдельной главы. Сейчас же хочется обратить внимание на то, что сетевой аккаунт сам по себе представляет ценность, и его

утрата может быть очень болезненна психологически, а иногда и финансово.

Сетевой аккаунт сам по себе представляет ценность, и его утрата может быть очень болезненна психологически, а иногда и финансово.

Всякому человеку жалко терять плоды своих трудов, даже если это всего лишь мемы и фотографии, собранные на его странице. Но главное даже не в этом — еще печальнее потерять те знаки внимания, которые вы получали от реальных и виртуальных друзей.

Во времена Пушкина социальных сетей не было, зато были альбомы, куда друзья и знакомые писали (то есть, выражаясь современным языком, «постили») шутки, мадригалы, признания в любви, запрещенные цензурой стихи, эпиграммы, шаржи, романтические рисунки и прочий, как бы мы сейчас сказали, «контент». И точно также «репостили» понравившееся из альбома в альбом, как мы это делаем сегодня. Причем альбомы были не только у чувствительных барышень или поэтов — их имели даже гусары и кавалергарды, как, например, граф Николай Толстой, отец знаменитого русского писателя. Расцвет «альбомной» культуры в России пришелся на 1820-е годы, потом мода постепенно прошла, оставив нам множество изящных и любопытных свидетельств той замечательной эпохи.

«Конечно, вы не раз видали
Уездной барышни альбом
Что все подружки измарали
С конца, с начала и кругом.

Сюда, назло правописанью,
Стихи без меры, по преданью

В знак дружбы верной внесены,
Уменьшены, продолжены...

...

...Тут непременно вы найдете
Два сердца, факел и цветки;
Тут верно клятвы вы прочтете
В любви до гробовой доски;

Какой-нибудь пиит армейской
Тут подмахнул стишок злодейской.
В такой альбом, мои друзья,
Признаться, рад писать и я...»[1]

Ну, скажите: чем это отличается от девчачьих страниц «ВКонтакте»?

Может быть, мода на соцсети тоже пройдет, а цифровые археологи, изучая наше время, будут удивляться тому, как мы были наивны. Так что не спешите ругать своих отпрысков за увлечение этим, в общем-то , невинным занятием; за минувшие двести лет люди нисколько не изменились, только перешли с бумаги на цифровые носители. Один из творцов альбомной культуры, Василий Львович Пушкин, очень точно сказал, что «альбом есть памятник души» — в наши дни это определение с полным правом можно отнести к персональным страницам в соцсетях. Вот именно поэтому потеря контроля над своим аккаунтом может вызвать психологическую травму у подростка или даже у взрослого.

---

1 А.С. Пушкин «Евгений Онегин», глава 4.

В то время, как большинство пользователей соцсетей ведет свои страницы исключительно в личных целях, некоторые умудряются на этом неплохо зарабатывать. Причем, среди ударников креативного труда в соцсетях есть немало юных дарований, которые смогли монетизировать свою страсть к созданию публикаций и занимаются этим делом вполне профессионально. Разброс доходов в этой сфере значителен: одним едва хватает на мороженое, а другие оказываются главными добытчиками в семье и даже содержат своих родителей. Понятное дело, что о безопасности такой курочки, несущей золотые яйца, стоит позаботиться как следует, ибо охотников до чужого добра предостаточно.

> *Популярность в интернете может прийти внезапно: какой-то ролик вдруг набирает миллионы просмотров, и его автор однажды утром просыпается знаменитым. В тот же самый момент его аккаунт становится мишенью для атаки, и с очень высокой вероятностью будет взломан.*

Поэтому, начиная карьеру блогера, нужно сразу хорошенько подумать о безопасности своего аккаунта.

Авторские права на цифровые произведения

Обычные пользователи интернета редко задумываются об авторских правах на свои произведения, а зря. Ведь может так случиться, что у вас во дворе высадятся инопланетяне, и вы успеете их сфотографировать. Или ваш домашний питомец вдруг наберет

толпу поклонников, как кошка из Аризоны по кличке Соус Тардар, которую весь мир знает как Grumpy cat («Угрюмая кошка»). Она стала знаменитостью и начала приносить своим владельцам ощутимый доход, набрав в итоге более десяти миллионов подписчиков в соцсетях, — такая слава вполне конвертируется в деньги.

> *В цифровом мире каждый сам себе автор и сам себе издатель — даже маленькие дети делают контент. А каждый разумный автор должен позаботиться о защите своих прав. Пусть даже вы не зарабатываете миллионы — обидно, если кто-то сворует ваши произведения.*

Не отстают в производстве интернет-контента и учителя.

> *64-летний преподаватель физики из Одессы Павел Андреевич Виктор по использованию современных технологий опережает многих молодых коллег. Уже пять лет он снимает на видео свои уроки для учеников 7-11-х классов и выкладывает их на YouTube. Сейчас их смотрят русскоязычные зрители со всего мира: у канала учителя более 80 тысяч подписчиков, а общее число просмотров перевалило за 8 миллионов.*
>
> *Павел Андреевич вспоминает, что все началось со скайп-конференций, которые ему пришлось проводить для заболевших учеников в лицее, где он преподает. Затем он решил расширить аудиторию своих уроков и самостоятельно освоил для этого новые технологии.*
>
> *К Виктору часто обращаются с предложениями монетизировать его канал, но преподаватель от них отказывается. «Мне*

кажется, что две вещи должны быть бесплатными в этой жизни — лечение и обучение», — говорит он[1].

Такая позиция, безусловно, вызывает уважение. Если вы тоже решите сделать свой контент всеобщим достоянием, то это нужно специальным образом обозначить, потому что могут найтись люди, желающие заработать на ваших произведениях вместо вас.

Например, вы можете публиковать свои произведения под лицензией Creative Commons, которая используется, когда автор хочет дать другим людям право делиться и использовать созданное им произведение. Лицензии Creative Commons применяются ко всем работам, на которые распространяется авторское право, включая книги, пьесы, фильмы, музыку, статьи, фотографии, блоги и веб-сайты.

Программисты, в том числе и юные, тоже могут публиковать свои разработки под так называемыми открытыми лицензиями, которых существует несколько видов. Вообще говоря, в индустрии программного обеспечения движение в сторону открытого исходного кода (open source) становится мейнстримом; даже гиганты отрасли, такие как Microsoft и IBM, многие из своих продуктов выпускают под открытыми лицензиями.

Однако следует помнить, что свободная или открытая лицензия не означает, что «все вокруг колхозное, все вокруг мое» — есть правила, которые надо соблюдать. Уже упомянутая лицензия Creative Commons имеет шесть типов, отличающихся набором требований и ограничений.

---

1 *Посмотреть уроки П. Виктора можно здесь:* ***https://www.youtube.com/user/pvictor54/videos***

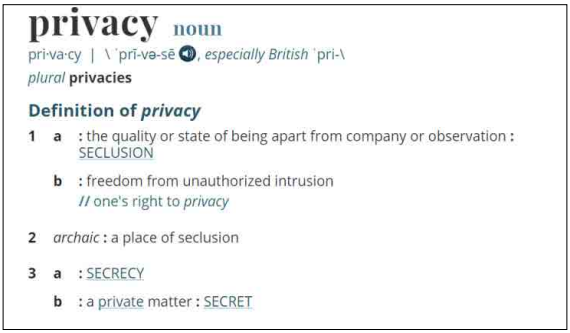
Заботясь о своих авторских правах, нужно уважительно относиться и к чужим. И помнить, что пиратский контент — часто источник вирусов, троянов и прочей заразы.

Заботясь о своих авторских правах, нужно уважительно относиться и к чужим. И помнить, что пиратский контент — это еще и источник вирусов, троянов и прочей заразы.

Тайна частной жизни

Представьте, что все стены вдруг стали прозрачными, все сказанное по секрету слышно всем, все, сделанное когда-то давно, помнится, как будто это было вчера. Представили? Это может показаться шокирующим, но мир сегодня действительно таков. Мы ежедневно попадаем в поле зрения сотен видеокамер, наши разговоры записываются, перемещения фиксируются. Мы добровольно променяли наши маленькие секреты на удобства, которые дают цифровые технологии. Ведь достаточно просто сказать: «О'кей, Гугл...», — и нужная информация тут как тут. Голосовые интерфейсы, такие как Алиса от «Яндекс» или Siri от Apple, становятся все популярнее, а это значит, что нас, вполне возможно, слышат 24 часа в сутки, запоминают и анализируют каждое наше слово.

В русском языке нет аналога слову «privacy», которое обычно используется в этом контексте в англоязычных странах. Прямой перевод дает варианты «конфиденциальность», «секретность», «уединение», «частная жизнь», но все они не совсем точно передают тот смысл, который мы находим в английском толковом словаре Merriam-Webster: «свойство или состояние быть вне компании



privacy noun

pri·va·cy | \ ˈprī-və-sē, *especially British* ˈpri-\

plural **privacies**

Definition of *privacy*

1 **a** : the quality or state of being apart from company or observation : SECLUSION

b : freedom from unauthorized intrusion
// one's right to privacy

2 *archaic* : a place of seclusion

3 **a** : SECRECY

b : a private matter : SECRET

или наблюдения» или «свобода от несанкционированного вторжения» И только потом — как архаическое значение! — идут «уединение» и «секретность».

Privacy вполне можно себе обеспечить и в цифровую эпоху, если относиться к вопросу технически грамотно. Оставьте дома свой мобильный телефон и пойдите погулять в лес — в нашем мире еще есть места, где вы не будете под присмотром Большого Брата и прочих любопытных глаз. А если вы находитесь в Сети, то будьте уверены — за вашими действиями наблюдают.

Если вы находитесь в Сети, то будьте уверены — за вашими действиями наблюдают.

Михаил Косински, в прошлом заместитель директора Центра психометрии Кембриджского университета, а в настоящее время доцент Стэнфордского университета США, говорит: «Вместо того, чтобы ввязываться в очередную битву за приватность, стоит признать, что война уже проиграна, и лучше озаботиться тем, чтобы мир стал благоприятной средой для человека, лишенного приватности».

В течение нескольких лет Косински с коллегами по Кембриджу разрабатывал систему, которая на основе активности пользователя в социальной сети составляет подробный психологический профиль человека. Система способна не только описывать особенности характера, но и предсказывать, среди прочего, пол, сексуальную ориентацию, цвет кожи и даже политические предпочтения пользователя. (Наработки Косински использовались фирмой Cambridge Analytica, якобы помогавшей Трампу победить на выборах. Правда это или нет, доподлинно неизвестно, но то, что попытки манипуляции мнением и даже поведением людей на основе сведений о них, полученных из интернета, делаются и будут делаться — это факт.)

Короче говоря, тайны частной жизни в том виде, как это было раньше, теперь не существует. Стоит ли этого опасаться? Вот, например, во многих европейских странах не принято иметь шторы на окнах — люди так и живут у всех на виду. О причинах возникновения этой традиции ходят разные легенды, но суть их одна: честному человеку нечего скрывать. Пожалуй, в нашем прозрачном мире это будет самое благоразумное решение: поменьше беспокоиться о том, что за вами наблюдают, и вести себя так, чтобы не было причин чего-то стыдиться.

- *В середине XVI века наместником Испанских Нидерландов был назначен жестокий Фернандо Альварес де Толедо, 3-й герцог Альба. За четыре года его наместничества было казнено более 18 тысяч мирных жителей. Среди многочисленных тиранических приказов герцога был запрет на закрытые шторами окна, поскольку голландцы часто устраивали домашние цеха по производству оружия и проводили революционные собрания. Спустя некоторое время король Испании отозвал Альбу из Нидерландов, революция победила, но традиция осталась в новом прочтении:*

теперь голландцы гордились, что им нечего скрывать, и их образ жизни соответствует христианским представлениям о морали.

- *В XVII столетии в Швеции был принят закон, запрещающий гражданам завешивать окна (кстати, документально он действует и по сей день, но является необязательным к исполнению). Закон был введен для того, чтобы каждый лично мог убедиться в том, что его сосед живет по средствам. Кроме того, во время обходов королевская стража имела право заглянуть в окна горожан, чтобы проверить, не нарушается ли порядок.*

- *Во Франции в период немецкой оккупации граждане, которые не сотрудничали с фашистами и не получали тем самым дополнительные пайки, держали окна открытыми, чтобы показать, что у них нет провианта от врага.*

Автор обескураживающей книги «Прозрачное общество» («The Transparent Society») Дэвид Брин приводит убедительные аргументы против тайны частной жизни.

Брин полагает, что чем упорнее мы пытаемся защитить нашу приватность, тем с большей долей вероятности ее потеряем. Он не предлагает, чтобы наши спальни стали открытой кормушкой для вуайеристов, но считает, что прозрачность дает нам возможность и право привлекать к ответственности тех, кто будет нарушать наши границы.

«Прозрачность — это не устранение частной жизни, — подчеркивает Брин. — Приватность подразумевает спокойствие дома и право быть в одиночестве», — пишет он[1].

1 *Is privacy possible in the digital age? // NBCNEWS.com, 7 декабря 2000.*

Но не надо путать приватность (конфиденциальность) и анонимность. Анонимность — это совсем другое дело, это желание скрыть свою личность при контактах с другими людьми или находясь на публике. Анонимность и раньше была проблемой: чтобы остаться неузнанными, люди переодевались в чужую одежду, носили маски, приклеивали бороды и усы — в общем, проявляли чудеса изобретательности, но весь этот карнавал отнюдь не гарантировал, что вас никто не узнает. А вдруг маска случайно спадет?

Также не стоит смешивать конфиденциальность с секретностью. Профессор Даниэль Вайцнер, директор Инициативы по исследованию политики интернета Массачусетского технологического института (MIT Internet Policy Research Initiative) и главный научный сотрудник Лаборатории информатики и искусственного интеллекта CSAIL, объясняет разницу между ними так:

> *«Существует мнение, что конфиденциальность и секретность — синонимы. И если вы можете хранить личную информацию в секрете, то это и есть конфиденциальность. Если же вашу личную информацию хранят третьи лица, то вы утратили всю свою конфиденциальность».*

Вайцнер отвергает такой подход. Он считает, что защита конфиденциальности в эпоху цифровых технологий означает создание правил, которые требуют от правительств и предприятий прозрачности в отношении того, как они используют нашу информацию[1].

---

1 *If There's Privacy In The Digital Age, It Has A New Definition // NPR.org, 3 марта 2014.*

Репутация в цифровом мире

Репутация — или, на французский манер, реноме — это «закрепившееся определенное мнение о человеке или группе людей», сообщает нам «Википедия». Как и в прежние времена, заработать хорошую репутацию все также трудно, а испортить ее все также легко — в этом смысле с приходом цифры ничего не изменилось.

Заработать хорошую репутацию все также трудно, а испортить ее все также легко.

Но есть одна важная деталь: люди по своей природе забывчивы, поэтому в прежние времена «все наши глупости и мелкие злодейства» могли сойти нам с рук. Теперь даже сущая ерунда, одно неудачное фото или резкая фраза могут если и не сломать жизнь, то хорошенько потрепать нервы, — люди очень по-разному понимают правила приличия и готовы затравить тех, кто, по их мнению, в эти правила не вписывается.

В фильме Алана Рене «Хиросима, любовь моя!» французская актриса приезжает в Японию на съемки и там знакомится с мужчиной-японцем. У них начинается роман, но суть не в этом: она впервые решается рассказать свою историю о том, как во время войны, будучи совсем молоденькой девочкой, влюбилась в немецкого солдата. Кончилось все печально: солдата убили, а ей не осталось другого выхода, кроме как бежать из своего родного городка в Париж, ибо репутация ее в глазах сограждан была загублена навечно. Хотя в чем она виновата? Судьба девушки и солдата почти в точности повторяет судьбу Ромео и Джульетты, с той только разницей, что на месте враждующих семей оказались враждующие страны, а «Джульетта» осталась жива. Что ждало ее, не решись она на побег? Ночной

разговор вдали от родины, на другом конце света, помог ей наконец-то пережить этот эпизод и найти силы жить дальше.

Если бы в 1945 году был интернет, то и в Париже героине не удалось бы скрыться. Обязательно нашелся бы какой-нибудь дотошный гражданин, который докопался бы до ее прошлого и окончательно поломал бы девушке жизнь. А уж в наше время то и дело встречаются бдительные товарищи, которые, как им кажется, стоят на страже общественной морали, хотя их никто на это место не назначал.

В январе 2019 года учительница из Барнаула разместила у себя в соцсети фото в купальнике. Сделала она это после заплыва в честь Универсиады в Красноярске, продемонстрировав свои медали и грамоту за участие в соревнованиях. Практически сразу вслед за этим учительница получила от директора школы настойчивое предложение уволиться: на нее пожаловалась мать одного из учеников, которой это фотография показалась вызывающей. История завершилась в целом благополучно: учителя по всей стране устроили флешмоб в поддержку коллеги и выложили фото в купальниках с хештегом #УчителяТожеЛюди; министр образования Алтайского края лично вступился за нее и предложил подыскать достойное место. Но учительница предпочла в школу не возвращаться.

Репутация — это не только сумма наших заслуг и проступков. Это еще продукт общественного мнения по их поводу, а нетерпимости и предрассудков и в наше время немногим меньше, чем в Средневековье. Что и говорить, мы не можем вести себя так, чтобы угодить всем тараканам в головах у разных людей, однако прежде, чем публиковать какие-то фото или что-то писать, стоит подумать о том, как это скажется на вашей репутации в будущем, ведь интернет не только пом-

нит все, он еще и сделал информацию доступной для всех и везде. И если раньше после какой-нибудь неприятной истории можно было переехать в другой город, где вас никто не знает, и начать жизнь с чистого листа, то теперь мы все живем в одной большой деревне под названием Земля, и деться с нее пока некуда.

Наверное, вы слышали про китайские эксперименты с социальным рейтингом, когда человеку за определенные проступки снижают баллы и, наоборот, поощряют за социально одобряемое поведение. Перевел бабушку через дорогу — заработал очко, не оплатил вовремя счета за коммунальные услуги — ушел в минус. А после некоторого порога начинают действовать ограничения: например, вам не продадут билет на самолет и придется добираться поездом в плацкарте. Можно по-разному относиться к этому эксперименту, но тенденцию он отражает точно.

> *Когда вся информация прозрачна, человеку надо осознанно относиться к управлению своей репутацией, и не важно, следит за ним какая-то государственная система или пока нет.*

Некоторые старшеклассники сами задумываются (и правильно делают) о том, что будущие работодатели обязательно посмотрят их страницы в соцсетях, и начинают более взвешенно принимать решения о том, что стоит публиковать, а что нет. Причем, нужно понимать, что полное отсутствие в Сети информации о человеке воспринимается как тревожный сигнал. Поэтому не стоит кидаться удалять свои страницы, если вам показалось, что они не соответствуют идеальному образу строителя цифрового будущего.

Так или иначе, не стоит забывать, что репутация — как осетрина: второй свежести у нее быть не может. А интернет только усиливает это свойство.

Переписка: почта и мессенджеры

Из тридцати томов полного собрания сочинений и писем А. П. Чехова письма составляют двенадцать томов — немногим менее половины всего им написанного.

> *Вступительный текст от редакции сообщает нам: письма Чехова представляют собой одно из самых значительных эпистолярных собраний в литературном наследии русских классиков. Всего сохранилось около 4400 писем, написанных в течение 29 лет, — с 1875 по 1904 год.*
>
> *Эти двенадцать томов — своеобразное документальное повествование Чехова о своей жизни и творчестве. Но познавательное значение его писем шире их биографической ценности: в них бьется пульс всей культурной и общественной жизни России конца XIX — первых лет XX века.*
>
> *Тематика эпистолярного наследия Чехова многообразна: от дневников путешествий и календарей работы над произведениями до событий личной жизни, литературных связей, от заметок об общении с театральными деятелями и отзывов на критику до советов начинающим авторам.*

В наше время бумажных писем практически никто не пишет, кроме как в официальные инстанции, да и те активно переходят на цифровые форматы. Но и в электронных письмах точно также бьется пульс эпохи и живут наши личные истории — любови, ссоры, обиды, бытовые дела, забавные глупости, просьбы, напоминания о встречах, планы, отчеты, претензии, благодарности, поздравления, офисные интриги и много-много рабочей рутины.

По объему переписки мы сегодня, пожалуй, превосходим Антона Павловича. Вот у меня, например, в почтовом ящике Gmail хранится более 8 тысяч отправленных писем, начиная с 2007 года. Я отнюдь не претендую на то, что мое эпистолярное наследие будет достойно изучения, однако потерять в одночасье весь этот накопленный багаж мне было бы жаль.

> *В письмах закопано много ценной информации — имена, адреса, телефоны, документы, интересные ссылки, важные договоренности, да и просто разные памятные моменты.*

Электронная почта сегодня не в чести, ее место заняли чаты и мессенджеры, но суть от этого не меняется: история общения с другими людьми все также представляет для нас ценность. Пусть даже почта как формат общения считается устаревшей, но адрес почтового ящика часто используется в качестве логина и для подтверждения различных действий. Например, если вы забыли пароль к какому-то сервису, то, скорее всего, для его восстановления вам на email придет специальная ссылка. Так что отправлять электронную почту на покой было бы преждевременно.

Это также хорошо понимают и хакеры, поэтому мы регулярно видим новости о массивных утечках паролей к электронной почте, а черный рынок услуг по взлому почтовых ящиков на заказ процветает. Если вы не какая-то знаменитость, то едва ли хакерам интересны ваши письма сами по себе. Но, покопавшись хорошенько в чьей-нибудь почте, можно выудить оттуда «явки и адреса» — параметры доступа к различным ресурсам, которыми человек пользуется. Поэтому к защите почтовых ящиков — как своих, так и детских — надо отнестись со всей серьезностью.

К защите почтовых ящиков — как своих, так и детских — надо отнестись со всей серьезностью.

Кроме того, рекламщики охотятся за «чистыми» почтовыми адресами, которые еще не засветились в спам-рассылках. Если им удастся заполучить ваш пароль, они с удовольствием будут рассылать от вашего имени свой мусор на адреса ваших друзей, да и просто случайным людям. Потом кто-нибудь пожалуется на спам и ваш ящик заблокируют.

С мессенджерами история аналогичная: формат изменился, но суть осталась прежней. То есть все, сказанное выше про электронную почту, применимо и к более современным каналам коммуникаций — Skype, WhatsApp, Viber, Telegram и др. Причем, благодаря большей интерактивности мессенджеров и эмоциональной вовлеченности, здесь чаще срабатывают банальные «разводки» — вроде такой, когда со взломанного аккаунта вашего знакомого просят срочно перевести деньги на какое-то важное дело. Увы, многие попадаются на эту удочку. Некоторые хозяева таких взломанных аккаунтов переживают подобные казусы настолько сильно, что готовы даже вернуть друзьям деньги, которые у них выманили злоумышленники, хотя их вины в этом нет. В любом случае, ситуация неприятная, и лучше подумать о защите, чтобы в нее не попадать.

Персональные цифровые коллекции

Еще совсем недавно по обычным меркам времени, то есть лет десять назад, мы старательно собирали свои цифровые коллекции музыки, фильмов, книг и программ, гордились ими, делились этими сокрови-

щами с друзьями и тщательно берегли. Причем делиться тогда значило не просто нажать кнопку «Поделиться», а взять с собой пустых болванок CD или DVD и поехать к другу домой, чтобы переписать себе что-нибудь интересное.

Сегодня интернет практически обнулил ценность таких персональных коллекций, если они только не содержат уж совсем эксклюзивные материалы. Нам стало проще погуглить, чем искать вдруг понадобившийся файл в своих закромах.

Кстати, в отношении к персональным цифровым коллекциям четко прослеживается граница поколений: «игреки» еще помнят, что это имело ценность, и по привычке держат подборки любимых фильмов и музыки на собственных носителях, а «зеты» твердо уверены, что в любой момент найдут все, что нужно, на каком-нибудь ресурсе в интернете. Поэтому вместо коллекции файлов теперь держат коллекции ссылок — это еще и более экологично: вместо сотен миллионов копий популярных видеоклипов на жестком диске или флешке, на YouTube есть всего одна копия, которую все могут посмотреть. (Технически копий исходного ролика больше, но по суммарному объему это все равно на много порядков меньше, чем было бы в личных хранилищах.)

> *Единственный вид коллекций, который с приходом тотальной цифровизации и вездесущего интернета не только не увял, а, наоборот, расцвел — это коллекции фотографий.*

Фотографируют теперь все, от мала до велика, и надо что-то с этим богатством делать, чтобы не потерять. О тех, для кого фотография стала серьезным хобби, можно не беспокоиться: они-то знают, как уберечь свои снимки от любых катастроф. А вот всем остальным не так оче-

видно, каким образом лучше организовать свой фотоархив. Память телефона забивается быстро, и хочешь не хочешь, а придется учиться копировать фотографии в облако — на сегодня это самое адекватное решение для обычных пользователей. Как ни странно, для многих это все еще представляет сложность, причем даже для юного поколения, которое с гаджетами на «ты».

Виртуальные вещи

Звонок в полицию: «Помогите! У меня украли танк!» — «Какой танк?!» — «ИС-4!»[1]

Вы, конечно же, догадались, что это был не настоящий танк, а виртуальный. Кто-то взломал аккаунт игрока в игре World of Tanks и угнал боевую машину. Несмотря на то, что танк виртуальный, потеря человека вполне реальна: игровое оборудование стоит немалых денег, и чужой танк можно продать, выручив за него кругленькую сумму.

> *По данным исследования Newzoo, российские геймеры за 2019 год потратили более 2 миллиардов долларов[2], а согласно прогнозу аналитического центра по игровой индустрии Superdata, Россия в 2020 году выйдет на третье место в Европе, потеснив Францию[3].*

---

1 *Похитители танков. // Российская газета, 16 сентября 2019.*

2 *The russian game market. // Allcorrect Group, 22 мая 2020.*

3 *Russia to Become the Third Biggest European Market for Video Games // Superdata, 22 ноября 2020.*

Пока с точки зрения российского законодательства виртуальные вещи, используемые в игровых мирах, имуществом не считаются, а это значит, что их присвоение не квалифицируется как кража. Тем не менее, иногда пострадавшие все-таки обращаются в полицию; бывает даже такое, что виртуальных воров находят и возвращают украденное хозяину. Для нарушителя наступает ответственность по ст. 272 УК РФ за неправомерный доступ к компьютерной информации как за деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности. Светит ему за это крупный штраф или даже реальный срок.

Очевидно, что в дальнейшем количество виртуального имущества будет только расти, и придется учиться принимать меры по его охране от всевозможных посягательств: будут развиваться способы безопасной продажи и обмена виртуальных вещей и так далее.

> *Масштабы некоторых сделок уже сейчас поражают воображение. Так, например, планета Calypso в игровой вселенной Entropia Universe была продана за 6 миллионов долларов. В той же вселенной космический курорт Club Neverdie нашел нового владельца за 635 тысяч долларов, а в игре Second Life за 50 тысяч долларов продали город Амстердам (точнее, его виртуальную копию). Еще одной из громких сделок стала продажа «эфирной розовой боевой собаки» (Ethereal Flames Pink War Dog) в игре Dota 2 (кстати, сейчас собачка подешевела и оценивается всего в 4 тысячи долларов).*

Потерять свои виртуальные богатства можно по двум причинам: либо кто-то взломал ваш аккаунт, либо вы захотели купить, продать или обменять какой-то предмет, а вам попался жулик. Чтобы уберечь аккаунт, следуйте стандартным советам: используйте

сложные пароли, никому их не передавайте, не используйте один и тот же пароль для почты и аккаунта Steam, включите дополнительную защиту Steam Guard, остерегайтесь фишинга, не забывайте про антивирус. Особенно будьте осмотрительны в контактах с незнакомцами — бывает, что кто-то предлагает вам поиграть за их команду на турнире и кидает ссылку на якобы голосовой чат, чтобы вы могли общаться, — а там оказывается стилер — программа, ворующая пароли.

Необязательно быть обладателем уникального артефакта. Злоумышленников интересуют аккаунты, стоимость инвентаря на которых составляет всего 5-10 тысяч рублей. Получив ваш пароль, они перехватывают управление, привязывают аккаунт к своей почте, а затем распродают ценный инвентарь или ищут покупателя на аккаунт целиком, если у вас достаточно «прокачанный» персонаж.

Кстати, по этой причине следует крайне осмотрительно относиться к покупке готового аккаунта — он вполне может оказаться краденым, и если через некоторое время его найдут, то вернут законному владельцу, а вас забанят. Несомненно, есть и добросовестные продавцы, но будьте бдительны.

Следует крайне осмотрительно относиться к покупке готового аккаунта — он вполне может оказаться краденым.

Вторая ситуация связана с риском мошенничества при сделках с игровым инвентарем. Для каждого из виртуальных миров существуют свои торговые площадки, где игроки обмениваются оружием, магическими предметами, украшениями и прочими вещами. Как и в реальном мире, например, на Avito, здесь можно

нарваться на жуликов — как на стороне продавцов, так и на стороне покупателей. И точно также есть риск, что вам «впарят» какую-нибудь бесполезную ерунду по цене самолета, — сделка пройдет без нарушений, но все равно вы останетесь обманутым.

К сожалению, эти виртуальные рынки еще слабо регулируются законодательством, так что надеяться здесь можно только на себя. Юристы работают над тем, чтобы ввести понятие «виртуального актива», что повысило бы правовую защищенность игроков, но что и когда им удастся сделать — неизвестно.

Контакты и заметки

В магазине канцтоваров все еще можно купить телефонные записные книжки, хотя это, скорее, дань традиции, чем товар повседневного спроса. Большинство таких книжек имеют формат А4 или А5, то есть представляют собой эдакий настольный вариант, а отнюдь не карманный. Карманные телефонные книжки тоже еще можно найти в продаже — некоторые в обложке из натуральной кожи, на хорошей бумаге и с золотым обрезом — отличный сувенир, ничуть не хуже берестяных грамот.

Реальной записной книжкой стал мобильный телефон, и сдавать позиции он не собирается.

А реальной записной книжкой стал мобильный телефон, и сдавать позиции он не собирается. Именно в телефоне у большинства людей хранятся все списки контактов и адреса, туда же заносятся важные заметки. К счастью, наши электронные записные книжки

в мобильных устройствах практически по умолчанию синхронизируются с облачными хранилищами Apple или Google (а может, и обоих сразу), так что потерять эти данные стало почти невозможно — если только вы специально не отключите опции резервного копирования.

Но при этом появляется другой риск — можно потерять контроль над своим аккаунтом, и тогда это будет большой проблемой, потому что все контакты тоже будут утеряны. (Есть еще соцсети, но пока еще это не 100-процентное перекрытие — не все наши контакты имеют профиль в соцсети.) Дублирующих записей на бумаге уже никто не ведет, наизусть телефоны не помнит (иногда даже свой собственный). То есть можно констатировать, что в части хранения контактов произошла полная цифровизация. Даже бабушки и дедушки, все еще опасающиеся смартфонов, держат личный телефонный справочник в своем старомодном мобильнике с кнопками.

Список контактов в телефоне — лакомая цель для хакеров. Заполучив его, они могут делать рассылки вашим знакомым от вашего имени.

Список контактов в телефоне — лакомая цель для хакеров. Заполучив его, они могут делать рассылки вашим знакомым от вашего имени, что сразу повышает уровень доверия к полученной информации (на самом деле — дезинформации), — и человек кликает на присланную ссылку или открывает вредоносный файл. Или того хуже: мошенники начинают просить помощи от вашего имени, а ваши доверчивые друзья переводят им деньги. Чаще всего это срабатывает с самыми близкими людьми, особенно с нашими пожилыми родственниками.

Домены (имена сайтов)

Регистрация доменного имени (то есть названия сайта) в среднем стоит около 500 рублей в год. Но это имя может стать очень дорогим активом и яблоком раздора, если оно прибрело в интернете популярность. Как вы думаете, сколько стоит домен apple.com? Даже предположить трудно. Короткий или запоминающийся интернет-адрес может стоить тысячи или даже миллионы долларов.

Короткий или запоминающийся интернет-адрес может стоить тысячи или даже миллионы долларов.

Говорят, Facebook* заплатил 8,5 миллионов долларов за покупку домена Fb.com в 2010 году, а сколько он стоит сейчас, можно только гадать. Впрочем, такое уже не продается, как и «Мона Лиза» Леонардо да Винчи. Название сайта становится важной частью идентичности компании, и его утрата может иметь катастрофические последствия для бизнеса. Из-за доменов порой разгораются настоящие баталии.

Так случилось в штате Айова в 2017 году[1]. Вооруженный пистолетом мужчина по имени Шерман Хопкинс ворвался в дом 26-летнего веб-предпринимателя Итана Дейо и потребовал перенести домен doitforstate.com на другой аккаунт. Завязалась борьба, Дейо был ранен в ногу, но в итоге

---

* *Соцсеть признана экстремистской и запрещена на территории РФ.*

1 *Сейчас сайт doitforstate.com закрыт. Его имя «Do it for state» — «Сделай это для штата (или страны)» — популярный мем, появившийся в Университете штата Айова. Возможно, у преступника были на него свои планы, но органы следствия не дали об этом информации.*
The Guy Who Robbed Someone at Gunpoint for a Domain Name Is Getting 20Years in Jail. // Vice.com, 15 июня 2018.

получил контроль над огнестрельным оружием и несколько раз выстрелил Хопкинсу в грудь. Нападавшего удалось спасти, он в итоге предстал перед судом и получил 20 лет тюрьмы.

До стрельбы в Айове дело дошло впервые, но кража (или, как говорят «угон» домена) — дело вполне обычное. Кража доменного имени происходит, когда злоумышленник подделывает регистрационные данные жертвы и передает домен другому человеку, отнимая его, таким образом, у законного владельца и приобретая над ним полный административный и операционный контроль.

Причины, по которым это становится возможным, все те же: слабые пароли, шпионское ПО и социальная инженерия. Если вы были слишком беспечны, и преступнику в результате удалось действовать от вашего имени, то доказать, что это были не вы, будет трудно. Краденые домены часто «отмывают», устраивая серию передач между новыми владельцами и запутывая следы. К сожалению, регистраторы и полиция редко помогают в таких ситуациях, потому что доменные имена не рассматриваются как физическая собственность.

Впрочем, случаются редкие исключения. Альберт Ангел купил сайт P2P.com за 160 тысяч долларов в июле 2005 года в качестве инвестиций, но год спустя сайт был украден. Альберт сообщил о краже в полицию Майами-Дейд, и к нему отправили офицера. В результате следствие вышло на Дэниела Гонсалвеса, 25-летнего компьютерного специалиста из Нью-Джерси, и обвинило того в краже P2P.com путем взлома почтового аккаунта Ангела. В 2011 году Гонсалвес признал себя виновным и был приговорен к пяти

годам тюремного заключения. Этот случай считается единственным уголовным приговором за кражу домена[1].

Но чаще всего и красть ничего не нужно. Владельцы просто забывают продлить регистрацию, и домен становится бесхозным. В такой момент его могут легко у вас перехватить, чтобы потом потребовать выкуп. Или просто ваш раскрученный домен купит кто-то другой и будет использовать для своего сайта.

Цифровые ресурсы

В больших городах почти у каждого в квартире есть wi-fi. Сегодня мы пользуемся безлимитным высокоскоростным интернетом, а еще не так давно трафик был достаточно дорогим, и каждый мегабайт был на счету. В то время процветал вид мошенничества, связанный с воровством трафика, — кто-то из технически продвинутых соседей взламывал ваш роутер и за ваш счет пользовался интернетом. Сейчас едва ли будет актуально ломать чужую сеть, чтобы сэкономить 300-500 рублей в месяц, но у хакера могут быть и другие мотивы: например, если он совершит какие-то противоправные действия через ваш роутер, то полиция и ФСБ, разыскивая его, придут к вам. Так что позиция по отношению к wi-fi «пусть пользуются все, мне не жалко» весьма уязвима — свои цифровые ресурсы нужно защищать.

Кроме канала доступа в интернет к цифровым ресурсам можно отнести место на дисках в облачных хранилищах, пакеты минут

1 *When Hackers Steal A Web Address, Few Owners Ever Get It Back // Huffington Post, 29 сентября 2014.*

и SMS на телефоне, подписки на кино и ТВ и так далее. В результате взлома ваших аккаунтов вы рискуете все это потерять. Скажем, некто может получить доступ к вашему личному кабинету мобильного телефона и продать ваши накопленные гигабайты интернета на бирже, как это позволяет делать Tele2.

Автомобиль

Про автомобиль Tesla говорят, что это компьютер на колесах. Так оно и есть. И весь мировой автопром уверенно катится в том же направлении — ко все большей компьютеризации транспортных средств. Бортовой компьютер есть во всех современных машинах, а пройдет немного времени — и все автомобили, едущие по дорогам, окажутся подключенными к интернету. Зачем это нужно? Вовсе не ради того, чтобы передать картинку на экран навигатора, — с этим справляется и обычный смартфон. Прежде всего, подключенность нужна для повышения безопасности движения. Подключенный автомобиль будет оперативно обновлять свои управляющие программы и сообщать производителю технические параметры систем и агрегатов, а тот, в свою очередь, на основе статистических данных, собираемых со всех машин, сможет прогнозировать возникновение отказов и рекомендовать ремонт. В авиации это делается уже повсеместно, теперь очередь за автотранспортом.

У любой — даже золотой — медали есть обратная сторона.

Но у любой — даже золотой — медали есть обратная сторона. Наличие в автомобиле компьютера, который управляет всеми системами, да еще подключенного к Сети, делает такой автомобиль

приманкой для хакеров. «Взлом машины — это прямая угроза для жизни ее владельца. Если злоумышленник получил удаленный доступ к автомобилю, это значит, что он может включить или выключить любую систему в любое время: повернуть руль, нажать на газ или тормоза, выключить фары», — говорит эксперт «Лаборатории Касперского» Денис Легезо и в качестве примера приводит эксперимент американских исследователей со взломом Jeep Cherokee.

> *На момент начала атаки жертва хакеров ехала со скоростью 110 км/ч по автостраде в центре города Сент-Луис. «Пока два взломщика удаленно играли с кондиционером, радио и стеклоочистителями, я гордился своим самообладанием. И в этот момент они добрались до коробки передач», — пишет журналист Wired, который находился за рулем взломанной машины.*
>
> *Злоумышленники в результате получили контроль над акселератором и тормозной системой машины, а также стеклоочистителями и клаксоном. Для того чтобы удаленно управлять автомобилем, им понадобилось всего-то взломать мультимедийную систему Uconnect через сотовое соединение.*
>
> *«Таким образом можно добраться до машины, несущейся по шоссе где-то по стране, далеко от взломщика. Вот она, поворотная точка, после которой удаленный взлом автомобиля становится реальностью», — отмечает обозреватель издания.*

Этот эксперимент получил широкую огласку, и владельцы таких машин сильно обеспокоились. Автопроизводитель Fiat Chrysler оперативно исправил программное обеспечение, чтобы обезопасить

своих клиентов, и предложил им посетить дилеров для апгрейда ПО, либо скачать его с официального сайта компании. Но сколько еще уязвимостей наверняка прячутся в автомобильных системах?

Короче говоря, автомобили дружной толпой вошли в семью кибервещей, со всеми вытекающими отсюда плюсами и минусами.

Умный дом

Фантастика «тихой сапой» проникает в жизнь: наши дома все больше наполняются разнообразными умными устройствами, призванными сделать их уютнее, избавить нас от бытовых хлопот, волнений о том, выключен ли утюг, достаточно ли продуктов в холодильнике, и какой фильм посмотреть сегодня вечером. Умная дверь откроется сама, узнав вас по лицу или по голосу, термостат настроит комфортную температуру вашего жилища, подумав также и об экономии ваших финансов, а ваш ужин будет автоматически приготовлен и подан к столу роботом-поваром.

Система безопасности, позволяющая отслеживать появление посторонних людей и предметов, обеспечит ваше спокойствие, а также позволит вести удаленный видеоконтроль за маленькими детьми и пожилыми людьми. На случай длительного отъезда может включаться режим симуляции присутствия хозяина, чтобы не давать ворам повода нанести вам визит.

> *Пока настоящий умный дом — это дорогая игрушка для обеспеченных людей, но будьте уверены: революция в домашнем хозяйстве пройдет незаметно и быстро.*

Роботом-пылесосом и сейчас уже никого не удивишь, а скоро все новые модели бытовых приборов начнут выпускать со встроенными «мозгами».

Все эти устройства будут автоматически подключаться к домашнему центру управления. Инженерные системы зданий тоже стремительно умнеют, и неизбежно с какого-то момента в новых домах начнут устанавливать все необходимые датчики сразу при постройке.

В принципе, ничего особо фантастического в этом нет: концепция «умного дома» была впервые сформулирована в 1984 году Американской Ассоциацией Домостроителей, и, по сути, является развитием тенденции улучшения условий жизни при помощи техники, возникшей с появлением электрических приборов в начале 1900-х годов. С приходом в дом компьютеров появилась возможность наладить согласованное управление устройствами и системами, а интернет добавил к этому связь с внешним миром — и теперь у каждой кофеварки есть шанс заявить этому миру о себе.

Теперь у каждой кофеварки есть шанс заявить этому миру о себе.

Кстати, именно с кофеварок все и началось. В 1991 году появился первый веб-сайт, и тогда же в Кембриджском университете в Соединенном Королевстве впервые применили веб-камеру, чтобы наблюдать за работой кофеварки, которая находилась в одной из компьютерных лабораторий. Теперь ученые точно знали, когда подойти за свежесваренным кофе.

Рэй Брэдбери превосходно описал умный дом в коротком и жестком рассказе «Будет ласковый дождь...», опубликованном еще в 1950 году.

«В гостиной говорящие часы настойчиво пели: тик-так, семь часов, семь утра, вставать пора! — словно боясь, что их никто не послушает. Объятый утренней тишиной, дом был пуст. Часы продолжали тикать и твердили, твердили свое в пустоту: девять минут восьмого, к завтраку все готово, девять минут восьмого!

На кухне печь сипло вздохнула и исторгла из своего жаркого чрева восемь безупречно поджаренных тостов, четыре глазуньи, шестнадцать ломтиков бекона, две чашки кофе и два стакана холодного молока.

— Сегодня в городе Эллендейле, штат Калифорния, четвертое августа две тысячи двадцать шестого года, — произнес другой голос, с потолка кухни. Он повторил число трижды, чтобы получше запомнили. — Сегодня день рождения мистера Фезерстоуна. Годовщина свадьбы Тилиты. Подошел срок страхового взноса, пора платить за воду, газ, свет».

В рассказе все закончилось для людей плохо: случилась атомная война и никто не выжил, а умный дом случайно уцелел и продолжал функционировать, как ни в чем ни бывало. (Похоже только, что у дома вышли из строя датчики присутствия хозяев — иначе зачем бы готовить завтрак, если никого нет?)

Однако совсем необязательно нужна глобальная катастрофа, чтобы внести разлад в слаженную работу маленьких автоматических помощников. Это могут сделать хакеры, и сценарий может оказаться хоть и не столь трагичным, как у Брэдбери, но весьма и весьма неприятным.

Вы подходите к двери, а она не открывается: система «забыла» ваше лицо и рисунок сетчатки. Конечно, вы понимали, что такое может случиться, поэтому у вас с собой всегда есть обычный ключ. Открыв дверь, вы неожиданно оказываетесь в темном помещении. Внутри холодно, потому что отопление не включилось за два часа до вашего прихода, как вы его запрограммировали.

Через несколько секунд начинает трезвонить умная сигнализация, считая, что в дом проник посторонний, хотя она должна была определить присутствие смартфона и отключиться. Наконец вы замечаете, что хоть что-то работает: телевизор включен. Но только показывает он странное: на экран выведено видео в реальном времени с умной камеры на потолке, следящей за вами. А за окном слышны сирены мчащихся к дому пожарных и полиции. Да что же такое стряслось? Ничего особенного, все просто: ваш умный дом кто-то взломал.

Подобного развития событий можно ожидать, если кто-то получит доступ к контроллеру, который управляет всеми приборами и устройствами вашего умного дома. Эксперт «Лаборатории Касперского» Владимир Дащенко показал на выставке Mobile World Congress 2018, что сделать это довольно просто[1], и такой сценарий вполне вероятен. Дело в том, что при разработке систем умного дома их авторы много думали о комфорте и почти совсем не думали о безопасности, поэтому взламываются они относительно легко (по сравнению, например, с банковскими системами).

1 *Апокалипсис в умном доме // Блог Kaspersky Daily, 28 февраля 2018.*

При разработке систем умного дома их авторы много думали о комфорте и почти совсем не думали о безопасности.

Тем не менее, оснований для паники нет (ну, или пока нет): умные дома еще не стали мишенью для массовых атак злоумышленников, потому что не очень понятно, какую выгоду из такой операции можно извлечь. Допустим, кто-то получил контроль над вашей умной лампочкой и теперь балуется, включая и выключая свет, когда ему вздумается. Чтобы прекратить атаку, вам достаточно вывернуть эту лампочку и вкрутить обычную. Аналогичным образом можно поступить и с остальными приборами — просто перейти на ручной режим, пока проблема не будет устранена. Все же обычный дом — не атомная станция, в нем нет таких систем, вмешательство в работу которых может иметь серьезные последствия. Максимум, чего добьются хакеры своими действиями, — вашего раздражения временными неудобствами.

Поэтому они предпочитают действовать другим образом: получив контроль над устройствами умного дома, формируют из них ботнет[1], с помощью которого могут в любой момент организовать DDoS-атаку.

Именно так и случилось в октябре 2016 года, когда без доступа в интернет осталась большая часть пользо-

1 *Ботнет — это набор компьютеров или умных устройств, подключенных к интернету, — «ботов», которые находятся под удаленным управлением какой-либо внешней стороны. Обычно эти компьютеры скомпрометированы злоумышленником, который управляет их функционированием без ведома владельцев.*

вателей на Восточном побережье США. В атаке участвовали миллионы устройств, она была столь масштабной, что власти готовы были заподозрить действия враждебного государства, но, как потом выяснилось, на самом деле это была работа гигантского ботнета Mirai (по-японски — «будущее»). В отличие от других ботнетов, которые обычно состоят из компьютеров, Mirai включал в себя множество устройств так называемого «интернета вещей» (IoT) — цифровых камер и видеопроигрывателей. Потом появились ботнеты, в состав которых входят роутеры, «умные» лампочки, розетки, датчики движения, выключатели, камеры наблюдения и другие гаджеты — настоящие пехотинцы DDoS-атак, которые просто-таки бомбардируют веб-трафиком целевой сервер до тех пор, пока он не будет перегружен и автоматически отключен. По состоянию на август 2019 года в интернете насчитывалось почти 27 миллиардов таких «вещей», и большинство из них может стать легкой добычей хакеров[1].

Персонально для владельца умного дома это опасности не представляет: ну, подумаешь, ваша лампочка посылает запросы на какой-то сервер! Хозяин лампочки за ее действия ответственности не несет (правда, если сумеет доказать, что это не он ее так запрограммировал). И уж коль скоро уязвимость домашних умных устройств (не только лампочек, естественно) попала в фокус внимания, то какое-то решение проблемы будет найдено, и производители начнут выпускать более защи-

1 *Number of Internet of Things (IoT) Connected Devices Worldwide 2020: Breakdowns, Growth & Predictions // Finances Online, 2019.*

щенные модели. В общем, нет серьезных причин отказываться от благ цивилизации из-за наличия подобных угроз.

Но одно исключение, пожалуй, есть: камеры видеонаблюдения.

> *Шалости хакеров могут быть отнюдь небезобидны, если они получат доступ к видеопотоку из вашего дома. В лучшем случае они выложат ролики со взломанных камер на YouTube, чтобы получить свою минуту славы. Но если взломщик узнает ваши персональные данные, то у него может появиться желание шантажировать вас под угрозой публикации видео.*

Этому риску чаще подвергаются известные люди, хотя и обычные граждане от него не застрахованы.

Иногда ситуация принимает более угрожающий характер. Однажды хакеры взломали видеокамеру на ноутбуке, который стоял в комнате маленького ребенка. Родители ставили ему на ночь мультики, ребенок засыпал, а компьютер потом сам переходил в спящий режим. Все было хорошо, пока мальчик не стал жаловаться, что в его комнате кто-то есть и разговаривает с ним. Родители сначала не поверили: ну да, все дети боятся темноты и воображают невесть что! Но ребенок плакал и ни за что не хотел оставаться в своей комнате. Хорошо, что взрослые все-таки поняли, что происходит нечто ненормальное, и отнеслись к словам малыша внимательно. Оказалось, действительно кто-то развлекался тем, что пугал ребенка по ночам: видя через камеру, что мальчик уснул, включал зловещие звуки и показывал на экране страшные картинки. А ког-

да малыш бежал звать взрослых, тут же все гасил, — и ребенку, естественно, не верили. Такое «баловство» может довести и до серьезного невроза.

Современные IP-камеры, используемые в системах домашнего видеонаблюдения, оснащены также микрофоном и динамиком, поэтому они вполне могут быть использованы в подобных сценариях — совсем необязательно, чтобы в детской комнате стоял настоящий компьютер.

К сожалению, на текущий момент риск взлома видеокамер остается высоким. Чтобы его свести к минимуму, нужно следовать довольно простым правилам:

- Во-первых, всегда обновлять прошивки камер и ставить сложные пароли для доступа к ним, а заодно почаще эти пароли менять. Как это сделать, обычно описано в руководстве пользователя каждой такой камеры. Это минимальные необходимые меры защиты;

- Во-вторых, всегда отключать неиспользуемые функции. В первую очередь это касается разнообразных «облачных» сервисов, которыми оснащается все большее число камер;

- В-третьих, если вы достаточно хорошо подкованы в техническом плане, можно сделать еще кое-что. Например, включить HTTPS-доступ к камере[1].

1 *Веб-камера против человека. // Блог Kaspersky Daily, 20 февраля 2017.*

Контрольные вопросы

1. Назовите, что ценного есть у вас в цифровом виде.
2. Какими способами преступники крадут цифровые деньги?
3. Зачем воровать мили и бонусы?
4. Чем опасны утечки персональных данных?
5. Почему нам так дороги наши аккаунты в соцсетях?
6. Как защитить свои авторские права в интернете?
7. В чем разница между конфиденциальностью и анонимностью?
8. Как заботиться о своей цифровой репутации?
9. Храните ли вы старые электронные письма и сообщения? Почему?
10. Какие у вас есть цифровые коллекции?
11. Есть ли у вас виртуальные вещи? Как их могут украсть?
12. Почему списки контактов для нас ценны? Зачем они хакерам?
13. Что такое доменное имя? Почему оно имеет ценность?

14. Почему надо защищать свой wi-fi?

15. Что хакеры могут сделать с компьютеризированным автомобилем?

16. Чем хакеры могут угрожать умному дому?