Как современные устройства собирают информацию о своих владельцах и какие способы помогают защититься от утечки данных

Советы от компании «СёрчИнформ» — российского разработчика средств информационной безопасности для компаний из разных отраслей.

Смартфон и компьютер — незаменимые помощники, с которыми прочно связано понятие повседневного комфорта. Прогноз погоды, такси и транспорт, обмен сообщениями, кино, работа и средство оплаты — приложения стали необходимыми.

Но даже если вы используете технологические блага не больше, чем среднестатистический россиянин, ваши данные — будь то счёт в банке, переписка или другая личная информация — под угрозой. Разберёмся, чем вы рискуете и как избежать неприятностей.

Угроза 01.Телефон и мобильные приложения

Производителю смартфона вы интересны только как владелец продукции — конкретные личности ему не нужны. Он хочет знать, где и когда вы впервые активируете телефон, чтобы отслеживать рынки сбыта для поставок запчастей и обеспечения сервисной поддержки. Ещё производителю важно понимать, какие функции вы используете, а какие – нет, чтобы развивать продукт.

Вот что обычно сообщают смартфоны своему производителю:

- марку и модель телефона,
- время и место активации (GPS, LBS или просто город),
- оператора связи,
- количество установленных SIM-карт и всю информацию про них,
- программы, установленные пользователем,
- статистику использования смартфона – разговоры, запуск отдельных программ и т.д.

Вся информация обезличена: производитель не понимает, кто есть кто, так что действия вроде бы законны. Но есть свои подводные камни.

В большинстве телефонов сохранено более 10 учётных записей от различных сервисов. Без подключения к ним и выхода в интернет смартфон — вещь практически бесполезная: его можно смело заменить обычным кнопочным телефоном. Поэтому если человек покупает смартфон, он сразу устанавливает нужные ему приложения через «магазины» и при первом включении создаёт учётную запись в Apple или Google.

Эти аккаунты — отличный способ идентификации, потому что производители операционных систем следят именно за личной информацией — «цифровой тенью» каждого пользователя.

Разработчики хотят знать, где вы любите ужинать и что планируете покупать, чтобы показать персонализированную рекламу. И если вашу учётную запись взломают, то вы своим данным больше не хозяин. Даже если производитель операционной системы чист на руку, его самого могут

взломать, чтобы украсть аккаунт. А следовательно — получить доступ ко всем данным. Например, к мобильному кошельку.

С мобильными приложениями дело обстоит ещё хуже. Такая простая программа, как «Фонарик», при установке может запрашивать доступ к местоположению, фотографиям, камере, микрофону и данным о подключении Wi-Fi — типичный пример действий недобросовестного разработчика. Если вы по неосторожности дали приложению доступ к этой информации, то оно может в любое время, даже когда фонарик выключен, собирать данные:

- определять местоположение,
- открывать, изменять и иначе использовать фото и другие файлы на телефоне,
- взаимодействовать с социальными сетями и облачными хранилищами,
- делать фотографии и снимать видео,
- записывать окружающие звуки,
- проверять, к какой Wi-Fi сети подключено устройство

При этом для работы фонарика нужен только светодиод, установленный внутри вспышки. Некоторые приложения требуют ещё больше: они хотят просматривать телефонную книгу, звонить контактам, читать сообщения и почту.

В апреле 2017 года случился скандал с приложением Unroll.me. Сервис обещал пользователям почистить их ящики от спам-рассылок и другого мусора за пару кликов. И выполнял обещание, но при этом тайно продавал их личные данные другим компаниям. Основательница Unroll.me не смутилась и сказала, что использовала единственный вариант монетизации бесплатного приложения.

Как защититься?

Смартфоны

Не включайте root-режим (Root – режим дает доступ к системе Android с правами администратора.), не делайте jailbrake (операция[1], которая позволяет получить доступ к файловой системе ряда моделей устройств iPhone, iPod или iPad) – это инструменты разработчиков, а не способ бесплатной установки платных программ.

Производитель, оператор связи и даже некоторые продавцы предустанавливают программное обеспечение (ПО) на смартфоны. Постарайтесь разобраться, что это за ПО и какова его функциональность. Ненужное удалите, если устройство это позволяет.

Защититесь не только от технологических, но и от человеческих рисков: включите авторизацию телефона по паролю или отпечатку пальца.

Приложения

Проверяйте авторство приложений и устанавливайте только официальные программы. По возможности, с качественным описанием, большим количеством скачиваний и высокой оценкой.

Следите за разрешениями, которые запрашивают приложения. Если их больше, чем нужно для работы программы, не соглашайтесь.

Проверьте разрешения уже установленных приложений – и удалите те, что хотят подозрительно много. Внимательно относитесь не только к установке нового ПО, но и к обновлению текущего. Новая версия может требовать новые разрешения.

Покупайте ПО. Лицензионные программы лучше защищены и имеют меньше соблазнов монетизироваться за счёт ваших данных.

Отключите автосинхронизацию с облачными сервисами, кроме случаев, когда она действительно необходима.

Не пренебрегайте двухфакторной аутентификацией, при которой вас попросят дважды подтвердить, что вы — это вы. Например, на первом этапе вы должны ввести логин и пароль, на втором — код из смс или электронной почты.

Угроза 02.Ваш компьютер и действия в интернете

В реальной жизни мы привыкли соблюдать правила: уходя из дома — закрывать дверь, прежде чем открыть её — смотреть, кто там.

Эти правила справедливы и для интернета. Там тоже есть мошенники, которые могут вам навредить. Например, получить доступ к интернет-банку и украсть все деньги или получить персональные данные и «повесить» кредит. Мошенники действуют через социальные сети, почту, привычные жертвам сайты или облачные хранилища. Их цель — ваши данные.

Фишинг

Один из самых популярных способов «выудить» личные данные пользователя. Мошенники практикуют это, используя разные каналы:

Электронное письмо из банка

Вы открываете и читаете неожиданное сообщение о том, что на ваше имя был оформлен кредит и на данный момент задолженность не погашена. Во вложении – договор займа и судебный иск, с которым вам предлагают ознакомиться и решить проблему. Письмо оформлено в корпоративном стиле банка с логотипом и в узнаваемом дизайне. Но если скачать вложения, на компьютер установится троян-шпион или вымогатель. Первый будет отсылать мошеннику всю нужную информацию, а второй заблокирует компьютер и предложит заплатить за разблокировку машины.

Другой вариант: вам сообщат о зачислении средств и попросят подтвердить платёж. Для этого вы должны перейти по ссылке и ввести

реквизиты карты. Открывшийся сайт тоже будет очень похож на оригинал, но, как и в письме, где-то затаится ошибка: например, в адресной строке или имени отправителя будут перепутаны буквы. Мошенники надеются, что вы этого не заметите.

Сообщение от друга

Хакеры взламывают аккаунты людей в социальных сетях или на площадках по интересам. Потом они рассылают френд-листу сообщение с просьбой одолжить денег (и отправить их на счёт). Как вариант – предлагают оценить забавную шутку, перейдя по ссылке с вирусом. В обоих случаях доверчивость может обойтись жертве в копейку.

Предложение онлайн-магазина, турфирмы или авиакомпании

«Поздравляем! Вы стали участником розыгрыша и победили!» – может сообщить вам известный бренд и предложить забрать свой подарок, бонус или скидочную карту. Для этого вам нужно перейти по ссылке и указать персональные данные. Дальше события будут развиваться по описанной выше схеме. Суть мошенничества одна, но рычаги давления разные: сделать заманчивое предложение, запугать или попросить помощи.

Сайты, маскирующиеся под настоящие

Вы хотите перевести деньги родителям и заходите в мобильный банк. Вроде бы всё как обычно, но на самом деле вирусы в фоновом режиме подменяют ваши действия своими. Зачастую отследить это можно только благодаря смс-уведомлениям банка. Если вы невнимательно прочтёте текст и не проверите назначение платежа и адресата, введёте код подтверждения, деньги уйдут не вашим родителям, а на счёт мошенников.

Перехват данных

Угрозу несёт и привычка подключаться к публичным Wi-Fi-сетям, будь то сеть в кафе, библиотеке или просто незащищённая паролем сеть на улице. Если в это же время в кафе сидит хакер, он может украсть данные двумя способами:

Прослушивание незащищённых соединений и перехват «открытых» данных

Когда вы открываете почту, пишете пост на форуме или загружаете документ в облако, весь проходящий трафик может сканироваться на наличие незашифрованных данных. Найденные учётные записи сохраняются и впоследствии используются злоумышленниками. Отсутствие зелёного значка в браузере – верный признак, что вы рискуете поделиться своими данными с мошенниками.

Создание поддельной страницы авторизации и перехват зашифрованных данных

Существует ещё один распространённый вариант перехвата данных. Хакер раздаёт бесплатный Wi-Fi, но с одним условием: при первом подключении к сети вы соглашаетесь использовать ненадёжный сертификат. Выбор прост: вы либо принимаете сомнительное предложение и пользуетесь бесплатным интернетом, либо отклоняете его и не получаете доступ в сеть. Вот что происходит, если вы соглашаетесь: защищённое соединение всё же

устанавливается, но не между вами и искомыми сайтами, а между хакером и этими сервисами. С этого момента пересылка любых данных и даже логин с паролем доступны хакеру вплоть до того момента, пока вы их не поменяете.

Дальнейшее развитие событий зависит от полученных данных и целей злоумышленника. Например, он может шантажировать тем, что расскажет боссу о сливах рабочей информации, узнает, по каким дням вы получаете зарплату или когда уедете в отпуск и оставите квартиру без присмотра.

Как защититься?

Проверяйте ссылки, прежде чем переходить по ним. Ошибка в названии сайта – гарантия того, что вас обманывают. И будьте бдительны: даже если сообщение пришло от знакомого, помните, что его могли взломать.

Регулярно меняйте пароли от всех используемых сервисов.

Подделать письма от вашего банка, турфирмы или другой организации не стоит большого труда. Если сомневаетесь в отправителе — позвоните на номер компании, который использовали для связи раньше, и выясните, действительно ли они отправляли вам письмо.

Если браузер предупреждает о небезопасном соединении — уходите с сомнительного сайта. И ни в коем случае не соглашайтесь на применение ненадёжных сертификатов шифрования.

Прежде чем вводить логин и пароль, убедитесь, что соединение защищено: перед адресом сайта должен быть префикс https («s» — значит secure — «безопасное», «зашифрованное»).

Обходите подозрительные сайты и ничего с них не скачивайте.

Критично относитесь к любым бесплатным сервисам и «выгодным» предложениям.

Если пришлось воспользоваться открытой сетью, убедитесь, что точка доступа принадлежит кафе, а не хакеру. Кафе по законодательству обязано идентифицировать пользователей, поэтому попросит вас ввести номер телефона и вышлет смс для входа.

Используйте шифрованное VPN-подключение для доступа в сеть. Оно не защитит от вирусов, фишинга и социальной инженерии, но зашифрует данные, которые вы передаёте, и убережёт от нечестных провайдеров и соседей в чужой сети.

Угроза 03. Фитнес-браслет и другие умные вещи

Если вы носите фитнес-браслет или недавно купили телевизор с голосовым управлением, значит приобщились к интернету вещей — системе

привычных, но имеющих доступ в сеть устройств. «Умные» вещи обмениваются информацией через интернет и работают без вмешательства человека. Это удобные девайсы, но проблема в том, что производители имеют к ним доступ, а мошенники могут его перехватить.

Возьмём «умный» телевизор: он в фоновом режиме слушает всё, что происходит в комнате. Это нужно, чтобы техника различала, когда человек говорит по телефону, а когда – даёт команду. В политике безопасности производители прямо заявляют: «Если в ваших словах содержится личная или другая частная информация, то она окажется среди полученных [телевизором] данных, которые будут переданы третьей стороне». Остаётся только догадываться, кто может стать этой третьей стороной.

«Дружественные» к шпионам технологии фитнес-трекеров позволяют мошенникам подключаться к браслетам без ведома владельцев. Частота вашего пульса мало кому интересна, но проблемы всё равно могут возникнуть: мошенники перехватывают контроль над девайсом и блокируют его. Хотите вернуть — платите. Это справедливо не только для бюджетных фитнес-браслетов, с дорогими смарт-часами дела обстоят так же.

Ещё одна плохая новость: умные браслеты умеют отслеживать движения рук, а мошенники успешно учатся их распознавать. Если схема движения вашей руки при наборе ПИН-кода в банкомате попадёт к хакерам, есть опасность, что они вычислят комбинацию. К этому пришли учёные Технологического института имени Стивенса из США. И хотя нет подтверждений того, что хакеры уже использовали эту хитрость, мы не можем быть уверены, что застрахованы.

Умных вещей становится всё больше, они повышают качество жизни, но в то же время — привносят новые угрозы. Интернет вещей — единственная сфера, где бессмысленно соблюдать «цифровую гигиену», чтобы защитить себя.

Вся суть технологии в постоянном обмене данными: вы либо соглашаетесь с рисками, либо отказываетесь от устройства. Оценить изнутри защищённость облачных сервисов пользователь не может. Эта забота ложится на плечи производителей, но в ваших силах изучать возможности гаджетов и отказываться от тех, которые хотят слишком многого или не гарантируют безопасность.