В зоне риска каждый

Эксперты в вопросах кибербезопасности считают, что полностью обезопасить себя от киберугроз не могут даже те, кто не пользуется интернетом. В 2015–2017 годах интернет-преступники доказали, что научились воздействовать на объекты инфраструктуры, например на линии электросети или на поезда метрополитена. А владение смартфонами, использование мессенджеров и банковских карт, применение технологий «умных» домов многократно увеличивают эти риски.

«Облака» в опасности

Так называемые облачные сервисы (возможность хранить данные в интернете, на серверах, расположенных в разных странах, например Dropbox, iCloud, «Яндекс.Диск») таят опасность как для крупных компаний, так и для обычных людей. Эксперты уверены, что в 2018 году мы столкнемся с ростом количества утечек данных из «облачных» сервисов. «Преимущества „облаков“ очевидны — удобная обработка и хранение данных, доступ к ним из любой точки мира. Но существует и проблема: совершенно непонятно, каким образом данные будут обрабатываться, после того как их отправили на „облачный“ сервер, каким образом провайдер будет их защищать — или не будет вообще. Данные становятся бесконтрольными: после того как мы их отправили в „облако“, они нам не принадлежат. Если раньше в зоне риска были пользователи почтовых сервисов, то сейчас „облачными“ сервисами начали пользоваться корпорации — и этим они сами загоняют себя в ловушку».

Корпорации ловят на удочку

В компании Positive Technologies считают, что еще одной угрозой для больших компаний становится фишинг (от английского fishing — "рыбалка"). Вам приходит обычное электронное письмо, в котором вам предлагают скачать некий файл, мотивируя это бонусом или приказом руководства. В этом файле находятся не только безобидные данные, но и зловредный код, который через ваш компьютер проникает в корпоративную сеть и начинает заражать другие компьютеры. Несмотря на то, что эту технологию применяют уже много лет, она не теряет своей актуальности у мошенников.

При этом защититься от фишинга сложно — к каждому пользователю компьютера не приставишь надзирателя. Однако, по мнению Юнусова, избежать потерь все же можно, если рассказать сотрудникам о том, как отличить фишинговое письмо от обычного, а также использовать программное обеспечение, которое позволит обнаружить зловредную программу на ранней стадии.

Большие данные — большие проблемы

Эксперты в области кибербезопасности опасаются и так называемых больших данных — сбора персональных данных, который происходит зачастую без вашего ведома и автоматически. "Многие компании — браузеры, поисковики, сервисы электронной почты, социальные сети — собирают информацию об интернет-привычках пользователей, они это делают для того, чтобы выдавать ему релевантные рекламные предложения. Получается двоякая штука: с одной стороны, «большие данные» — это хорошая штука, потому что она помогает улучшать качество сервисов и делать их релевантными для пользователей. С другой стороны, если эти данные попадут в руки мошенников, они могут более эффективно использовать против человека методы социальной инженерии.

Рассмотрим пример: вы приобретаете в магазине, например, одежду и выкладываете об этом пост в социальную сеть. Через некоторое время по номеру телефона, который вы указали в своем профиле, перезванивает незнакомец, представляется сотрудником банка и говорит, что при покупке такого-то товара в таком-то магазине деньги с вашего счета списались в двойном объеме. Для возврата средств на счет вас просят назвать номер карты и кодовое слово либо CVC\CVV-код (три цифры на задней стороне карты), а также набор цифр из подтверждающей эсэмэски. Этих данных достаточно, чтобы через легальный интернет-банк перевести деньги с вашей карты на счет злоумышленника.

Ульянов говорит, что схожий сценарий возможен и в случае, если вы не публикуете информацию о своих покупках в интернете: «Сейчас сбором „больших данных“ занимаются не только банки, но и розничные магазины. В отличие от кредитных учреждений, которые всегда относились к информационной безопасности серьезно, ретейлеры защищают данные гораздо хуже».

«Умные» вещи и человеческий фактор

Проникающие в нашу жизнь «умные» вещи часто становятся пособниками хакеров. Холодильник, который заказывает товары сам и публикует пост в соцсетях, если его открывают после 23, «умный» дом, который обогреет или освежит квартиру до приезда хозяев, автомобильные сигнализации с управлением через смартфон и даже автопилот — все это, безусловно, делает нашу жизнь проще и комфортнее. Все такие устройства имеют сим-карты с доступом в интернет и могут «общаться» между собой. Злоумышленники используют их для создания ботнетов — сетей, состоящих из таких «бессловесных» устройств, которые могут атаковать какой-либо сайт и сервис и вызвать его перегрузку. Такие атаки называются DDoS — распределенная атака типа «отказ в обслуживании». «Эти вещи не особо защищены, потому что их производитель уделяет внимание безопасности в третью очередь — в первую очередь это удобство для пользователя, красивый интерфейс и тому подобное. Они часто имеют стандартные заводские настройки. Эти вещи легко взламываются, и их можно использовать для создания бот-сетей.

Одним из факторов риска остается простая человеческая лень: покупатель «умной» техники просто не меняет установленный на заводе пароль — чаще всего это стандартное сочетание 123456 или слово password. Иногда пароль изменить просто невозможно — его устанавливают на заводе, и его также просто взломать.

Хорошая новость в том, что большинство «умных» вещей имеют физическую блокировку от нанесения вреда своему хозяину. Поэтому поджарить "умный" дом при помощи отопительного котла, управляемого со смартфона, злоумышленники, скорее всего, не смогут.

Как защититься?

Если хакеры захотят получить доступ к вашим данным, они его получат. Другое дело, что рядовой пользователь вряд ли интересен хакерам международного уровня. А рядовому пользователю нужно соблюдать правила «информационной гигиены», и тогда, скорее всего, ему удастся избежать опасности.

1. Электронная почта

Зачем защищать: Через фишинговые письма хакеры могут установить зловредную программу на ваш компьютер.

Как защищать:

Не скачивайте файлы, которые вам прислали по электронной почте, если есть хоть какие-то сомнения в том, что они отправлены человеком, которому вы доверяете. Чтобы удостовериться, свяжитесь с отправителем другим способом (по телефону или в мессенджерах) и уточните, отправлял ли он вам сообщение с приложенным файлом.

Проверяйте адреса отправителя: злоумышленники часто создают почту, адрес которой похож на адрес доверенного отправителя, например, меняют между собой буквы i и l.

Перед выполнением инструкций, отправленных по электронной почте, уточните у руководителя, действительно ли он их давал, например, позвоните ему по телефону.

2. Смартфоны

Зачем защищать: Вредоносные приложения могут из-за ошибки пользователя получить права «суперпользователя» и рассылать опасный код по всем Wi-Fi-сетям, к которым подключается телефон. Кроме того, некоторые приложения могут записывать и передавать ваши персональные данные.

Как защищать:

Устанавливайте приложения только из официальных магазинов — AppStore, Play Market, Windows Store.

Не разрешайте приложениям использовать те устройства, которые им, по вашему мнению, не нужны: например, если игра просит доступ к управлению телефонными звонками — это повод насторожиться.

По возможности разделяйте функционал устройств, например, если вы активно используете смартфон для интернет-серфинга, в том числе по подозрительным сайтам (онлайн-игры, сайты «для взрослых») или часто подключаетесь к незнакомым Wi-Fi-сетям, то не рекомендуется использовать этот же телефон для интернет-банкинга или входа в закрытую корпоративную сеть.

Если вы очень переживаете за конфиденциальность информации, относитесь к устройствам так, будто их уже взломали. Кроме того, многие телефоны собирают данные об истории вашей геолокации — если хотите, чтобы они оставались строго конфиденциальными, отключите трекинг. Однако это может привести к сбою в полезных программах вроде «Найти мой телефон» или навигационных приложениях.

3. Социальные сети и мессенджеры

Зачем защищать: Данные, размещенные в открытом доступе, можно использовать для мошеннических действий. Через социальные сети и мессенджеры злоумышленники могут украсть у вас деньги, используя методы социальной инженерии.

Как защищать:

Старайтесь не выкладывать в открытый доступ номер телефона.

Посты, по которым можно восстановить ваш адрес и привычки, старайтесь выкладывать так, чтобы их могли видеть только люди, которым вы доверяете.

Подключите двухфактурную аутентификацию — после ввода пароля к своей странице вам придет СМС с кодом, который нужно ввести. Злоумышленнику будет намного сложнее получить доступ к вашему профилю.

В случае, если ваш друг в социальной сети или мессенджере просит вас перевести деньги или сообщить какие-то личные данные, убедитесь, что его страница не взломана: задайте ему несколько вопросов, ответы на которые не может знать злоумышленник (например, место, где он с вами познакомился). Кроме того, лучше перезвонить по телефону и уточнить, действительно ли это сообщение писал ваш приятель.

Не вводите пароль от своего профиля в соцсети на сторонних сайтах.

Не используйте одинаковые пароли к компьютеру, почте, разным соцсетям.

PIN и CVC/CVV-коды вашей банковской карты не сообщайте никому, даже близким друзьям и родственникам. То же самое касается кодов подтверждения банковских операций, которые вы получаете в СМС.

Обязательно выходите из своего аккаунта после работы на чужом компьютере, а по возможности старайтесь даже не логиниться на устройствах, принадлежащих не вам.

4. "Интернет-вещи"

Зачем защищать: Принадлежащая вам «умная» вещь может стать частью бот-сети, созданной для кибератак.

Как защищать:

Если производитель позволяет это, сразу после покупки изменить пароль доступа к вашей «умной» вещи на секретный.