Информационная безопасность: как нащупать границу между паранойей и разумной предусмотрительностью? (Часть 1)

Мы много раз рассказывали о том, какими многочисленными и изощрёнными угрозами полон интернет, как много желающих заполучить ваши деньги и личную информацию, насколько хитёр и изворотлив их преступный ум, а потому опасности подстерегают буквально на каждом шагу. Только «вошли» в интернет – и вот вы уже почти физически чувствуете, как персональные данные утекают к сидящему на «том конце» злобному хакеру! Хотели помочь беспризорным детям, нажали на ссылку – и все данные на компьютере зашифрованы, и вы точно знаете за сколько получите их обратно (или не получите)! Через аэропортовый «вай-фай» лишь на 5 минут зашли в интернет-банк «положить на телефон» оплату роуминга – счёт пуст!

Сначала удивляешься, даже любопытно становится – как это случилось? Как смогли, шельмы? Потом даже наступает какая-то жалость к самому себе: ну почему именно со мной? Затем уже волной подкатывает раздражение и злость: врёшь – не возьмёшь!

Тут не каждый сдюжит.

Как не «перегнуть палку» в следовании рекомендациям «безопасников»? Как не превратиться в вечно всего боящегося параноика, но стать действительно «твёрдым орешком» для злоумышленников – осведомлённым и думающим пользователем, уместно и умело применяющим эффективные средства и методы защиты?

У многих из нас, «безопасников», как ни странно, есть друзья и знакомые. И у многих из нас эти самые друзья и знакомые посмеиваются, слыша советы наподобие «не размещать немедленно в соцсетях фото места, где сейчас находишься» или «заклеивать «глазок» веб-камеры ноутбука, если она не используется». При этом высказывается аргументация от «Это в принципе невозможно!» до «Да кому я нужен?!». И наши ответы «Возможно» и «В этом-то и проблема, что такой вполне может найтись, но ты об этом даже не узнаешь», в общем-то, радикально ситуацию не меняют. Потому что антагонизм контролирующего исполнение и исполняющих будет всегда.

Какими же принципами резонно руководствоваться при определении необходимости тех или иных защитных мер, а также при выборе средств защиты?

1. Не стоит недооценивать киберпреступников – вы просто можете не всё знать. Если об угрозе говорят уже многие («безопасники», друзья, СМИ) – для этого, обычно, есть повод и совсем не стоит проверять реальность угрозы на себе. И через веб-камеры месяцами скрытно наблюдали за ничего не подозревающими пользователями, и банковские счета после пользования незащищёнными беспроводными сетями «чистили». Всё это – сегодняшняя реальность, и отрицать возможность того, что вы будете следующим, опрометчиво. Хотя, конечно, и не повод для паранойи.
2. Будьте осведомлённым в вопросах информационной безопасности пользователем. Нет необходимости (а у многих и возможности) становиться профессионалом и вникать во все детали вопросов защиты от современных киберугроз. Но «быть в курсе», иметь представление о существующих «напастях» современного цифрового мира и знать, как и чем от них защищаться – для этого, поверьте, действительно не требуется много времени и средств. Зато наверняка однажды сослужит вам хорошую службу (причём вы об этом можете даже не узнать – и к счастью!).
3. Стоимость защиты не должна превышать возможный ущерб в случае прорыва защиты. Иными словами, игра должна стоить свеч: нет смысла приобретать мудрёные средства шифрования и делать по 3 резервных копии данных, которым цена – копейка. Целесообразность никто не отменял.

В следующих частях мы подробно рассмотрим 8 защитных мер, из-за применения которых окружающие могут посчитать вас параноиком, и почему данные меры следует считать не паранойей, а разумной предусмотрительностью.

Информационная безопасность: как нащупать границу между паранойей и разумной предусмотрительностью? (Часть 2)

В этом и следующем выпусках мы рассмотрим несколько примеров того, как кажущиеся на первый взгляд явно чрезмерными меры обеспечения информационной безопасности на второй взгляд представляются необходимыми в современных реалиях проявлениями разумной предусмотрительности.

1. **Использование разных email-адресов для различных целей.** Зачем же усложнять? Почему нельзя использовать один email-аккаунт для всех и всего? Не надо запоминать несколько паролей и к какому аккаунту каждый из них подходит, не надо каждый раз задумываться какой адрес давать родственникам, друзьям, при регистрации на форумах и даже для пересылки рабочих документов. Удобно же! Наверно, мы не откроем Америку, если скажем, что удобство сегодня часто идёт в ногу с риском: чем удобнее, тем рискованнее с точки зрения безопасности. Используя один email-адрес «для всего», вы повышаете риск взлома сразу всей вашей переписки вместе со всеми конфиденциальными и не очень данными, которые неизбежно содержатся в email-сообщениях. Хорошей практикой является использование одного email-адреса для, например, подписки на рассылки, другого – для регистрации в онлайн-магазинах, третьего – для общения с родственниками и хорошими знакомыми и даже четвёртого – для иных нужд. Также никогда не следует использовать один email-аккаунт и для рабочей, и для личной переписки.
2. **Создание нескольких резервных копий очень важных данных - минимум трёх, причём хранящихся в разных местах на различных физических носителях.** Данный совет берёт свои корни из практики обеспечения непрерывности деятельности компаний. У каждого из нас есть данные или материалы, безвозвратная потеря которых крайне нежелательна – например, семейный фото- и видеоархив за много лет, или собственноручно собранная профессиональная база данных документации с предыдущих мест работы. Поэтому ценность 1) резервного копирования и 2) многократного резервного копирования почему-то начинаешь особенно ясно понимать только когда плод многолетних усилий бесследно исчезает, оставляя тебя ни с чем. Почему именно три копии? Считается, что три копии позволяют снизить риск утери до приемлемой величины в соотнесении с затратами на создание и поддержание в актуальном и исправном состоянии всех копий. При этом необходимо иметь ввиду, что у каждого места хранения копий есть свой средний «срок службы»: владелец облачного хранилища может подвергнуться хакерской атаке с потерей всех данных клиентов, да и просто может прекратить своё существование; внешний жёсткий диск может сломаться или стать мишенью вирусов; DVD-диски можно поцарапать и они перестанут «читаться». К слову, самым надёжным хранилищем данных по сей день считается старая добрая ленточная библиотека.
3. **Заклеивание «глазка» веб-камеры ноутбука.** Мы уже писали об этом: регулярный шпионаж за вами с помощью вашей же веб-камеры – довольно частая реалия современности. Примеров тому множество, причём как со стороны злоумышленников-одиночек, удалённо наблюдающих за жизнью своих «жертв» из любопытства, так и со стороны организованных групп, целенаправленно собирающих информацию о нужных им людях с целью вымогательства. Своё дело знают и спецслужбы государств (тут, конечно, вспоминаются телекраны из Оруэлловского «1984»).
4. **Неразмещение в открытом доступе фотографий своих детей.** Да и своих фотографий тоже. Потому что вы никогда не знаете (и не узнаете), кто и с какой целью может просматривать или хранить эти фотографии, и как он будет их использовать (сейчас или через много лет). Были примеры, когда создавались «группы по интересам», целью которых было глумление над чужими фотографиями или же поиск изображённых на фото людей и их унижение с помощью фото.

Однажды «выпустив» информацию о себе в интернет, вы никогда не можете контролировать её распространение и использование, притом, что такая информация сразу становится доступной неограниченному кругу людей.

Информационная безопасность: как нащупать границу между паранойей и разумной предусмотрительнос-тью? (Часть 3)

Сегодня мы завершаем рассмотрение примеров того, как кажущиеся на первый взгляд явно чрезмерными меры информационной безопасности на второй взгляд представляются необходимыми в современных реалиях проявлениями разумной предусмотрительности.

5. **Неразмещение в соцсетях информации о том, где вы сейчас находитесь.** Сюда относится как прямое упоминание вашего местоположения, так и косвенные признаки, которые позволят узнать, где вы сейчас находитесь (например, ваши фотографии на фоне достопримечательностей). По крайней мере, пока вы не дома. Не следует сообщать неограниченному кругу неизвестных вам лиц о том где вы, и что дома вас нет – случаи, когда любители чуть ли не поминутно «постить» фотографии с маршрутов своих передвижений обнаруживали свои жилища «тщательно обследованными», далеко не единичны.
6. **Не уверен – не открывай!** Это касается как незнакомых ссылок (особенно так называемых «коротких» - вроде http://bit.ly/2sl0qEL), так и вложений в письма. Ибо вы никогда не знаете, куда или к чему приведёт нажатие на ссылку или на вложение – часто это может привести к переходу на фишинговый сайт или к автоматической загрузке и запуску вируса-шифровальщика. В данном случае любопытство, спешка и неосторожность могут сыграть с вами крайне неприятную шутку. Причём во многих ситуациях антивирус может не спасти.
7. **Поддержание используемого ПО в актуальном состоянии.** В любом ПО есть уязвимости, которые могут быть использованы злоумышленниками – вопрос лишь в том, кто быстрее их найдёт, производитель этого ПО или преступники. Первыми чаще оказываются последние. А ведь сегодня поддерживать регулярно используемое вами ПО в актуальном состоянии (то есть своевременно применять патчи и ставить обновления, выпускаемые производителем ПО) не так уж и сложно – большинство программ сами отслеживают наличие патчей и обновлений, и от пользователя требуется лишь подтвердить установку нажатием одной кнопки (а перед этим убедиться, что патч или обновление действительно предоставляются производителем ПО, а не злоумышленником). Поэтому сегодня погоня за новейшей версией ПО – не дань моде, а необходимость!
8. **Отказ от использования публичных беспроводных сетей для совершения критически важных операций.** Например, для использования интернет-банкинга или отправки конфиденциальных документов. Многие из нас полагают, что если за 5 минут «быстренько положить деньги на телефон», то никто ничего «не заметит» и «ничего не случится». Вполне может статься, что заметит и случится. И если не сразу, то несколько позже – вы никогда не знаете, кто тот «ботаник» в очках, что насуплено уставился в свой ноутбук через столик от вас в кафе, и что именно он делает.

К сожалению, большинство из нас достаточно легкомысленно воспринимает увещевания относительно информационных угроз, привнесённых в нашу жизнь современным развитием информационных технологий, и потому ограничивается, в лучшем случае, лишь базовым набором мер и средств обеспечения безопасности.

До первого серьёзного инцидента…