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.