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…