# 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.