

«Основные правила безопасности в сети Интернет»

Интернет – уникальная реальность нашего с вами времени. Это безграничный мир информации, где есть не только развлекательные и игровые порталы, но и много полезной информации для учебы. Здесь можно общаться со своими друзьями в режиме онлайн, можно найти новых друзей, вступать в сообщества по интересам. Информация, оперативно обеспечивающая ваши ежедневные потребности, - все это Интернет.

Почему же полицейские вынуждены предупреждать об опасностях виртуального мира, если в нем так много всего хорошего и полезного?

Достаточно большая часть интернет-пользователей ищет не друзей в Интернете, а свои жертвы.

Дело в том, что недобросовестные граждане - мошенники, наркоторговцы, иные злоумышленники, асоциальные и психически нездоровые люди по-своему оценили возможности Интернета. Ведь именно Всемирная паутина дает возможность преступникам действовать анонимно.

Поэтому небезопасное поведение в сети Интернет может нанести вред и вам, и вашим родным и близким людям. Обезопасить себя не так уж и трудно – достаточно серьезно отнестись к проблеме кибербезопасности и соблюдать простые правила.

ТРИ самых общих правила, которые в наш информационный век должны стать вашими спутниками на всю жизнь:

1. ПАРОЛИ (ключ от дома)

Используйте всегда индивидуальные и сложные пароли, состоящие из букв, цифр и специальных символов. Исключите использование паролей по умолчанию, не сохраняйте пароли в ваших гаджетах и браузерах. Почему мы говорим об этом в первую очередь? Статистика говорит о том, что люди мало уделяют внимания парольной политике.

Третий год подряд самым популярным паролем в мире является «123456». Подобрать такой пароль к вашим порталам и персональным данным злоумышленнику не доставит труда.

Регулярно осуществляйте смену паролей, обеспечивая каждый раз их конфиденциальность. Это ваш самый большой секрет, как ключ от замка входной двери в ваш дом.

Правило первое: «Ключ от дома должен быть секретным, надежным, и только вашим, личным».

2. ВИРУСЫ и АНТИВИРУСЫ («моем руки с мылом»)

Любому компьютеру или гаджету могут навредить вредоносные программы (или вирусы). Они могут скопировать, повредить или уничтожить важную информацию, отследить ваши действия и даже украсть средства со счета.

Программы «Черви», «Трояны», «Шпионы» - их множество разновидностей и красивых названий, а суть одна – все это вредные вирусы!

Для защиты компьютера на нем устанавливаются специальные защитные программы и фильтры. Использовать можно только лицензионное программное обеспечение с актуальными обновлениями.

Устанавливать надо все обновления, как только они становятся доступными. Нельзя допускать истечения срока действия вашего антивируса.

Не качайте программные продукты из сомнительных источников (файлообменных сетей и торрентов). Не открывайте и не сохраняйте подозрительные файлы – сразу удаляйте. Не отвечайте на непонятные вам рассылки.

И главное - не посещайте ресурсы с сомнительной репутацией, которые вызывают у вас (или у вашей антивирусной программы) подозрения любого толка. Сомневаетесь – не нажимайте «да» или «ENTER».

Здесь можно провести простую параллель – держимся подальше от вирусов, моем руки регулярно, хорошим и качественным мылом. При любой сомнительной ситуации: «Моем руки с мылом, к вирусам не прикасаемся».

3. ПЕРСОНАЛИЗАЦИЯ (документы в сейфе)

Никому не передавайте свои конфиденциальные данные (логин, пароль), свидетельство о рождении, паспортные данные, адрес и прописку, и даже ваши фотографии. Такие «цифровые следы», если их создать, могут тянуться за вами всю жизнь. Могут навредить вам на пути к достижению поставленной цели. Игнорируйте в сети Интернет подобные запросы.

Получается странно – дома и на работе мы храним свои документы в сейфе, закрываем на ключ. Мы понимаем их важность. А потом по непроверенному запросу открываем сейф, достаем документы, фотографируем и посылаем посредством ресурсов в сети Интернет. Количество лиц, которые могут получить доступ к таким посланиям, даже трудно прогнозировать.

Давайте запомним третье правило: «Наши документы всегда в сейфе».

