**«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, наркодилеры, 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».

**10 правил безопасного поведения**

**в интернете**

* Никогда не распространяться о личной информации — своей и семейной. Никому нельзя говорить свой адрес, адрес и номер Школы, свои настоящие фамилию и имя, имена родителей. Под запретом сведения о местах работы родителей, их трудовом графике. Никто не должен узнать, в какие часы ребёнок дома один или в квартире вообще никого нет. Фото, даже вполне приличные, отправлять тоже не стоит.
* Родителям, особенно в первое время, нужно следить за тем, какие сайты посещает ребенок. Если среди них есть подозрительные, то это повод провести беседу.
* Уделите внимание теме защиты от спама. Научите определять такие Сообщения и не отвечать на них, не переходить по подозрительным ссылкам.
* Придумайте и запомните хороший сложный пароль. Сообщите ребёнку, что его нельзя никому называть.
* Если выйти в Сеть пришлось с чужого устройства, потом обязательно стоит выйти из своих аккаунтов. Лучше ещё и почистить историю посещений.
* Нужно ограничивать время, которое ребенок проводит в Сети.
* Установите правило: перед продажей или покупкой в онлайн-режиме родителей нужно поставить в известность.
* Для начинающих блогеров особенно важно очертить круг запрещённых тем. Это все, что противоречит российскому законодательству, и, конечно, личные сведения.
* При использовании Инстаграма лучше никогда не указывать геолокацию. Конечно, это малореальное требование. Но вот местоположение домашних снимков нельзя отмечать точно.
* Нужно научиться определять фишинговые сайты. Ссылки на них часто приходят на электронную почту, но их можно и просто встретить в Сети. Такие сайты выманивают данные пользователей. Их адреса похожи на популярные веб-ресурсы, выглядят они как meil.ru, wk.ru, feisbook.com. Переходить по таким линкам опасно, как минимум, можно поймать вирус.

**Как распознать злоумышленника**

Вот по каким признакам можно узнать, что человек может оказаться преступником.

* Вы не знакомы с ним в реальной жизни.
* Есть основания думать, что это взрослый человек.
* В соцсети у него мало друзей или их нет вовсе.
* Он настойчиво просит собеседника о чём-то, даже, на первый взгляд, безобидном: отправить своё фото, рассказать о чём-то, встретиться.

Собственно, поведение в интернете не должно сильно отличаться от поведения в реальном мире. Тем же правилом могут руководствоваться родители: не нужно излишне контролировать детей, но и пускать все на самотёк недальновидно.

И ещё дети должны помнить, что все, с кем они общаются через экран, это незнакомцы. И намерения у них могут быть самыми разными. Даже если общение установилось и хочется считать его своим другом.