Правила безопасности в сети Интернет

Интернет – уникальная реальность нашего времени. Это безграничный мир информации, где есть не только развлекательные и игровые сайты, 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.

Но небезопасное поведение в сети Интернет может нанести вред, причем не только вам, но и вашим родным и близким.

Обезопасить себя нетрудно – достаточно серьезно отнестись к проблеме кибербезопасности и соблюдать простые правила.

Существуют три основных направления по обеспечению кибербезопасности:

- защита компьютеров и гаджетов от вирусов;
- кибермошенничество;
- нарушение морали и этики в онлайн-общении, троллинг, разрушающий ваше личное пространство.

При троллинге, или по другому ругани в сети, прежде всего не нужно отвечать на оскорбления, чего и хочет тролль, и, если есть возможность, занести человека в черный список, заблокировать. Также в соц. сетях есть возможность пожаловаться на тролля. Тогда уже им займутся модераторы сайта.

А теперь рассмотрим самые общие правила безопасности в сети Интернет:

Правило 1. ПАРОЛИ

Используйте всегда сложные и непохожие друг на друга пароли.

Пароли должны содержать:

- больше 7-8 символов, иначе их можно быстро подобрать простым перебором,
- буквы и цифры,
- заглавные и строчные буквы,
- русские и иностранные буквы,

- специальные символы, например, запятая или скобки.

Буквы в пароле не должны содержать слова на любом языке и в любом написании: русском, иностранном или транслите. Также не должно быть дат рождений.

Самыми популярным паролями в мире являются «123456», «123456789», «qwerty», «password», «11111111». Они взламываются мгновенно.

Исключите использование паролей по умолчанию. Нужно сразу их менять на свои.

Не сохраняйте пароли в ваших гаджетах и браузерах. Лучше для это использовать, например, записные книжки или тетради. Конечно должен быть ограничен доступ и к ним.

Регулярно осуществляйте смену паролей.

Запомните! Пароли - это ваш самый большой секрет, как ключ от замка входной двери в ваш дом. Поэтому первое правило звучит так: «Ключ от дома должен быть секретным, надежным, и только вашим, личным».

Правило 2. ВИРУСЫ и АНТИВИРУСЫ

Любому компьютеру или гаджету могут навредить вредоносные программы (или вирусы). Они могут украсть, зашифровать 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 отвечайте на непонятные вам почтовые рассылки или так называемые «письма счастья». Не жалея, и не сомневаясь удаляйте их. Никакого дедушкиного миллионного наследства за границей у вас не будет. И выигрыша в лотерею без вашего участия тоже. Установите фильтр электронной почты для блокирования спама.

Не качайте программные продукты из сомнительных источников. Для этого есть официальные сайты производителей программ или известные интернет-магазины. Например, Play Market.

Все скачанные файлы нужно проверять на наличие вирусов до их открытия.

И главное - не посещайте ресурсы с сомнительной репутацией, которые вызывают у вас (или у вашей антивирусной программы) подозрения любого толка. Сомневаетесь – закройте веб-страницу. Поищите другой более безопасный и известный сайт.

Защищенный сайт обычно имеет Интернет-адрес, начинающийся с https вместо http. И адрес он имеет соответствующий своей тематике, торговой марке или названию организации.

Здесь можно провести параллель с мытьем рук. При мытье рук с мылом руки будут чище, также и, установив антивирус, мы можем лучше защитить свое устройство от заражения вирусами. Поэтому второе правило звучит так: «Чтобы не было вирусов, моем руки с мылом».

Правило 3. ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Никому не передавайте свои персональные данные, такие как:

- логины/пароли,
- свидетельство о рождении,
- паспортные данные,
- адрес и прописку,
- и даже свои 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.

Чтобы предотвратить хищение денег с банковских карт родителей ни в коем случае нельзя разглашать номера карт и пин-коды. Рекомендуется включать оповещение по SMS о банковских операциях по картам.

Как дома или на работе мы храним свои документы в сейфе, закрываем на ключ, так и к своим персональным данным должен быть закрыт доступ других людей. То есть нельзя посылать и передавать документы по сети и защитить эти данные на компьютерах и гаджетах с помощью соответствующего компонента вашего антивируса.

Давайте запомним третье правило: «Документы должны лежать в сейфе».

Итак, чтобы обезопасить себя нужно быть осторожными в сети и соблюдать вышеприведенные правила. В других непонятных случаях, которые могут произойти, обращайтесь к родителям.