

ПАМЯТКА ДЛЯ ОБУЧАЮЩИХСЯ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Социальные сети — это один из самых востребованных ресурсов Интернета.

Благодаря им сделан огромный шаг вперед в деле информатизации общества.

Между тем, помимо огромного количества возможностей, интернет несет и проблемы:

1. Компьютерные вирусы, которые при скачивании могут повредить или уничтожить файлы и данные.
2. Сети Wi-Fi (открытые), подключаясь к которым, Ваши личные данные могут попасть 3-им лицам.
3. Социальные сети. Размещая какую-либо информацию, пользователь и не представляет, как она может быть использована.
4. Электронные деньги. Поскольку эти средства виртуальные, есть разные способы их украсть, будьте внимательны и осторожны с ними. **НИКОМУ НЕ СООБЩАЙТЕ ПАРОЛЬ ОТ ВАШЕЙ БАНКОВСКОЙ КАРТЫ.**
5. Электронная почта. Не стоит скачивать подозрительные файлы, особенно от неизвестных пользователей.
6. Кибербуллинг - это намеренные оскорбления, угрозы и сообщение другим компрометирующих данных с помощью современных средств коммуникации.

Для безопасной работы в интернете (сайты), необходимо соблюдать всего 5 простых правил:

1. Не скачивайте и не открывайте подозрительные файлы с непроверенных источников.
2. Не размещайте личную информацию, которую могут использовать против вас.
3. В интернете ведите себя вежливо, не оскорбляйте других пользователей, не проявляете агрессию.
4. Никому не рассказывайте свои банковские реквизиты (если у вас имеется банковская карта).
5. Создавая аккаунт где-либо придумывайте **СЛОЖНЫЙ** пароль, состоящий как из прописных и заглавных букв, так и из цифр, а также устанавливаете двойную аутентификацию.

Основные советы по безопасности в социальных сетях:

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты планируешь провести свободное время;
3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;

5. Избегай размещения фотографий, где ты изображен на местности, по которой можно определить твое местоположение;
6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда, если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Кибербуллинг или виртуальное издевательство

Кибербуллинг - преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

1. Не бросайся в бой. Лучший способ: посоветоваться, как себя вести и, если нет того, к кому можно обратиться, то вначале нужно успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;
2. Управляй своей киберрепутацией;
3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;
5. Соблюдай свою виртуальную честь смолоду;
6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;
8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщите взрослому, тому, кому доверяете, куратору, социальному педагогу.