Памятка по технике безопасности в социальных сетях

- Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей.
- 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 и твои родители планируете провести каникулы;
- 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;
- Используй настройки конфиденциальности аккаунта. Настрой просмотр содержимого твоей учетной записи "только для друзей". Таким образом, незнакомые люди не увидят твою личную информацию;
- Принимай запросы в друзья только от тех людей, которых ты знаешь и которым доверяешь;
- Не используй веб-камеру для общения с людьми, которых ты не знаешь;
- Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
- Будь осторожен - некоторые пользователи могут представляться кем угодно;
- Если ты действительно хочешь встретиться с человеком, с которым познакомился в интернете, то договорись о встрече в общественном месте и желательно взять с собой кого-то еще, например, друга. Если твой сетевой друг считает, что присутствие кого-то еще плохая идея, то стоит отказаться от встречи;
- Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
- При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
- 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;
- Не размещай фотографии и видео со своими друзьями без их разрешения. Обращайся к друзьям, чтобы они также соблюдали конфиденциальность и не размещали твои фотографии и видео в общем доступе;
- Никогда не открывай подозрительные ссылки, даже если они пришли от твоих друзей. Удостоверься в том, что друг тебе выслал эту ссылку сам, а его аккаунт не контролирует киберпреступник. После взлома аккаунта злоумышленники в первую очередь делают рассылку по адресной книге, а поскольку доверие друзей друг другу выше, то вероятность заражения вирусами резко вырастает;
- Чтобы попасть в свою социальную сеть или на какой-либо другой сайт лучше используй закладки или окно быстрого доступа. Таким образом, ты точно попадешь на те порталы, которые безопасны и которыми ты пользуешься. При наборе адреса есть риск того, что ты ошибешься с адресом и не заметишь этого.
- Никогда без ведома взрослых не отправляй СМС, чтобы получить информацию из интернета. Иногда всплывает окошко – очень яркое, даже мигающее, примерно с такими словами: «Только сегодня – уникальный шанс – участвуй и выигрывай!» Заманчиво, правда? Ты щёлкаешь на него и тут сообщение: «Для того, чтобы принять участие в розыгрыше тебе необходимо прислать СМС!» Остановись! Ни в коем случае не делай этого без ведома взрослых, ведь это могут быть мошенники. И одна, казалось бы, безобидная СМС-ка может стоить тебе больших денег.

Не забывай, что интернет – это не главное увлечение в жизни. Кроме него у тебя должны быть любимые книги, занятия спортом и прогулки с друзьями на свежем воздухе!