ПАМЯТКА ДЛЯ ОБУЧАЮЩИХСЯ

Дорогой друг! Запомни эти правила безопасности в интернете:

1. Всегда спрашивай родителей о незнакомых вещах в интернете. Они расскажут, что безопасно делать, а что нет.
2. Прежде чем начать дружить с кем-то в интернете, спроси у родителей как безопасно общаться.
3. Никогда не рассказывай о себе незнакомым людям. Где вы живете, в какой школе учитесь, номер телефона должны знать только ваши друзья и семья.
4. Не отправляй фотографии людям, которых ты не знаешь. Не надо чтобы незнакомые люди видели твои личные фотографии.
5. Не встречайся без родителей с людьми из интернета вживую. В интернете многие люди рассказывают о себе неправду.
6. Общаясь в интернете, будь дружелюбен с другими. Не пиши грубых слов, читать грубости так же неприятно, как и слышать. Ты можешь нечаянно обидеть человека.
7. Если тебя кто-то расстроил или обидел, обязательно расскажи родителям.

Как распознать злоумышленника?

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

1. Ты не знаком с ним в реальной жизни.
2. Есть основания думать, что это взрослый человек.
3. В социальной сети у него мало друзей или их нет вовсе.
4. Он настойчиво просит тебя о чём-то, даже, на первый взгляд, безобидном: отправить своё фото, рассказать о чём-то, встретиться.

Советы о защите персональных данных в социальных сетях:

1. Проявляй осторожность при переходе по ссылкам, которые вы получаете в сообщениях от других пользователей или друзей.
   Не следует бездумно открывать все ссылки подряд. Сначала нужно убедиться в том, что присланная ссылка ведет на безопасный или знакомый сайт.
2. Контролируйте информацию о себе, которую ты размещаешь. Обычно злоумышленники взламывают учетные записи на сайтах следующим образом: они нажимают на ссылку "Забыли пароль?" на странице входа в учетную запись. При этом для восстановления или установки нового пароля система может предлагать ответить на секретный вопрос. Это может быть дата рождения, родной город, имя мамы. Ответы на подобные вопросы можно легко найти в сведениях, которые ты опубликовал на своей странице в какой-либо популярной социальной сети. Поэтому при установке секретных вопросов нужно придумывать

их самостоятельно или стараться не использовать личные сведения, которые легко найти в сети.

3. Не думай, что сообщение, которое ты получил, было отправлено тем, кого ты знаешь, только потому, что так написано. Помни, что хакеры могут взламывать страницы и рассылать электронные сообщения, которые будут выглядеть так, как будто они были отправлены твоими друзьями. Если у тебя возникло такое подозрение, будет лучше связаться с отправителем другим способом. Например, по телефону, чтобы убедиться в том, что именно этот человек отправил сообщение. Точно также необходимо относиться и к приглашениям зарегистрироваться в социальной сети.
4. Чтобы не раскрыть адреса электронной почты своих друзей, не разрешай социальным сетям сканировать адресную книгу вашего ящика электронной почты.
5. Не добавляй в друзья в социальных сетях всех подряд. Мошенники могут создавать фальшивые профили, чтобы получить от тебя информацию, которая доступна только твоим друзьям.
6. Не регистрируйся во всех социальных сетях без разбора.
7. Проявляй осторожность при установке приложений или дополнений для социальных сетей. Многие социальные сети позволяют загружать сторонние приложения. Довольно часто такие приложения используются для кражи личных данных. Поэтому к их использованию необходимо относиться также серьёзно, как и к установке на свой компьютер программ, которые ты можешь найти в Интернете.
8. 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!