**Что угрожает детям в Интернете**

Современные дети много времени проводят в Интернете, поэтому важно научить их безопасному поведению в цифровом пространстве.

1. **Взлом учетной записи**

Если не защищать учётные записи, злоумышленники могут взломать их и использовать личную информацию. Например, шантажировать ребёнка фотографиями, фактами из переписки или рассылать от его лица просьбы о помощи или спам. А кража игрового аккаунта может стать ударом для подростков, увлечённых киберспортом.

1. **Сбор личной информации**

Некоторые подростки делятся на своих страницах в соцсетях подробностями частной жизни, чтобы произвести впечатление на друзей. Опубликованные фото квартиры с дорогой техникой могут привлечь грабителей, а фото из отпуска подскажет им, когда никого не будет дома.

1. **Фищинг-использование поддельных ссылок**

Мошенники могут использовать доверчивость детей и вынудить их перейти по фишинговым ссылкам на сообщения с информацией о выигрыше, выгодном предложении и другие. Злоумышленники создают поддельные сайты, чтобы похищать логины, пароли, платёжные данные. Также при переходе по фишинговой ссылке может загрузиться программа, которая заразит компьютер или гаджет вирусом.

1. **Кибербуллинг- травля в Интернете**

В цифровом пространстве дети могут подвергаться травле. Обидчик может быть анонимным, поэтому его сложно вычислить. Кроме того, виртуальные издевательства происходят в личной переписке и родители могут не узнать, что ребёнка преследуют. Последствия кибербуллинга для детей сравнимы с реальной травлей: негативные эмоции, депрессия, проблемы с учёбой

**Что делать родителям**

**Расскажите о правилах защиты учетных записей**

Прежде всего — это надёжный пароль. Он должен состоять не менее чем из 12 знаков, включать маленькие и заглавные буквы, цифры и специальные символы. Легко запомнить фразу, связанную с жизненной ситуацией, и превратить её в надёжный пароль, например, «Я\_люблю\_лето\_2024!»

Для каждого сервиса нужно использовать разные пароли, желательно менять их раз в полгода. Порекомендуйте ребёнку использовать подтверждение входа, например, ввод пароля и код доступа на телефон. Злоумышленник, сумевший добыть чужой пароль, не сможет попасть в учётную запись без одноразового кода из СМС.

* Используйте сложные пароли длиной 12 знаков, которые содержат заглавные и строчные буквы, цифры и специальные символы
* Используйте для паролей случайную комбинацию букв, цифр и других символов. Подойдут забавные фразы, которые нужно записывать буквами разного регистра и добавляя цифры и символы
* Не используйте для паролей личные данные или другую информацию, которую публикуете вы или ваши близкие в социальных сетях
* Храните пароли в специальных программах — менеджерах паролей
* Используйте разные пароли для каждой важной учётной записи
* Не храните пароли на бумажных носителях, в электронных блокнотах, заметках и браузерах
* Обязательно используйте подтверждение входа