Что рассказать детям о кибербезопасности

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

Что угрожает детям в интернете

1. Взлом учётной 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.

2. Сбор личной информации

Некоторые подростки делятся на своих страницах в социальных сетях 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.

3. Фишинг — 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.

4. 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

1. Расскажите о правилах защиты учётных 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_2025!».

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.

2. Поговорите о важности настроек приватности

Вряд ли дети согласятся полностью закрыть свою страницу от всех, кроме друзей, однако можно ограничить возможности других пользователей. Например, запретить посторонним присылать сообщения, комментировать посты и фотографии. Также можно настроить видимость постов: слишком личные оставить видимыми для друзей или только некоторых из них.

Объясните ребёнку, что он может блокировать пользователей, которые угрожают ему, оскорбляют или обижают.

3. Расскажите, что можно и что нельзя публиковать в социальных сетях

Не следует публиковать фото дорогих вещей, техники в квартире, тем более с геометками. Такие фото лучше оставить для личной коллекции. Даже если они были отправлены в сообщениях, такие фото могут стать предметом шантажа.

Кроме того, нельзя публиковать фото документов, билетов на концерт и другую конфиденциальную информацию. Всё это не стоит хранить даже в закрытых постах или альбомах, потому что в случае взлома учётной записи или самого сервиса данные окажутся в руках мошенников.

4. Научите распознавать фишинг

Главное правило - не переходить по ссылкам из сообщений, которые пришли от подозрительного отправителя. Типичные признаки фишинга - выгодное предложение, информация о выигрыше. Иногда мошенники имитируют рассылки от настоящих сервисов или интернет-магазинов. В этом случае их можно определить по некорректному адресу отправителя. Часто он вообще не соответствует подлинному, а иногда отличается от него одной или двумя буквами, например, admin@notify.wk.com вместо admin@notify.vk.com.

5. Попросите не пользоваться важными приложениями при подключении к бесплатному вайфаю

Часто публичные сети плохо защищены. Иногда мошенники сами создают точки доступа, которые выдают за бесплатный вайфай кафе или парка. Благодаря этому злоумышленники перехватывают и могут подменить любую информацию, в том числе логины и пароли от учётных записей и платёжную информацию.

6. Расскажите об опасностях интернета

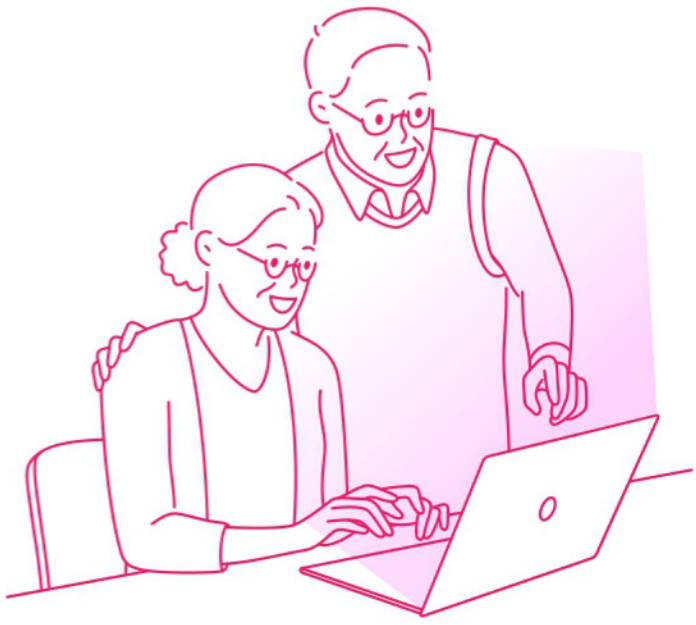
Дети часто воспринимают виртуальную среду как более безопасную по сравнению с реальной. Но в интернете надо соблюдать те же правила, что и в реальной жизни: не общаться с незнакомыми людьми, не доверять им и рассказывать обо всём родителям. Не стоит посещать сомнительные ресурсы, скачивать пиратские программы или медиаконтент.

7. Объясните, что в интернете нужно быть вежливым

Это поможет не провоцировать агрессию. Если ребёнок стал объектом кибербуллинга, можно заблокировать обидчика и сообщить о происходящем администраторам соцсети. Негативный комментарий может появиться под любой публикацией. Объясните ребёнку, что к нему это не относится и подобные комментарии нужно игнорировать или отвечать на них юмором

Как создать надёжный пароль 3

- Задайте пароль длиной 12 и более символов
- Используйте верхний и нижний регистр, числа и специальные символы
- Используйте случайные комбинации
- Откажитесь от простых комбинаций букв и чисел — qwe123
- Не берите за основу публичную информацию: девичью фамилию матери или дату рождения
- Используйте фразу, которая связана с жизненной ситуацией и легко запоминается, например «Я_обожаю_эклеры_с 10_лет!»



Информация, которую нельзя раскрывать по телефону 1

Персональные данные

- ФИО
- Адрес регистрации или проживания
- Данные документов: паспорта, СНИЛС, ИНН

Банковские данные

- Номер карты
- Три цифры на обороте (CVV-код)
- Список последних операций по карте
- Коды из смс- и пуш-уведомлений
- Кодовое слово
- Остаток на счёте

Фразы, которые говорят только мошенники 2

- Назовите номер вашей карты
- Назовите код из смс от вашего банка
- В каких банках вы ещё обслуживаетесь?
- Сколько средств у вас на счёте?
- Рядом с вами сейчас находится кто-то? Для банка они являются третьими лицами и не допускаются к операции
- Назовите ваш логин и пароль
- Какое у вас кодовое слово?
- Ваш сын попал в беду, а вы бросаете трубку. Вы не хотите ему помочь?