Не верь рекламным объявлениям

Никто не защищен от мошеннических действий, даже взрослые. Иногда требуется слишком много времени, чтобы понять, что перед тобой обманщик. Однако есть четкие признаки подозрительных и опасных сайтов: обилие яркой рекламы на странице, «кричащие заголовки», предлагающие «прямо сейчас» и «бесплатно» – такой информации в сети доверять не следует.

Чтобы убедиться, что информация не несет вреда и соответствует действительности, можно сравнить ее в других источниках, а также уточнить у родителей и друзей, стоит ли доверять опубликованному.

Опасайся незнакомцев

Конечно, если вы уже не первый месяц играете с сетевым другом в онлайн-игру и немного друг друга знаете, никто не помешает вам с ним весело проводить время. Однако если незнакомый человек назойливо стучится в личные сообщения, отвечать на них не стоит. Постоянные обращения, частые письма, просьбы прислать свои данные и фото – это повод прекратить общение, заблокировать человека и рассказать о произошедшем взрослым.

Используй только официальные сайты

Фишинг – способ, который используют мошенники для выманивания личных данных через интернет. Происходит это так: пользователь получает ссылку, похожую на адрес соцсети или почтового сервиса, переходит по ней, вводит на поддельном сайте конфиденциальные данные и становится жертвой злоумышленников. Система автоматически устанавливает вредоносные программы на устройство и крадет персональные данные.

Чтобы этого не произошло, важно внимательно проверять все, что вам присылают, прежде чем переходить по ссылкам. Обращайте внимание на детали, проверяйте адрес сайта, на который вам предстоит зайти. Чаще всего разница заключается в одной букве: например, для mail.ru может быть создан meil.ru, а для vk.com – vc.com.

Отличай поддельные аккаунты

В интернете любой может придумать себе личность – проверить информацию не так просто, как кажется. Это затрудняет распознавание тех, кто скрывается под фейковым именем. Подделку отличить все-таки можно, и вот основные ее признаки:

- **минимум друзей или их отсутствие;**
- **страница обычно только что созданная и пустая;**
- **незнакомец постоянно соглашается, указывает на вашу с ним схожесть;**
- **назойливость, не готовность прерывать разговор;**
- **большая разница в возрасте – взрослый человек не должен настойчиво набиваться в друзья детям.**

Соблюдай правила сетевого этикета

Не груби, будь вежлив даже в тех случаях, когда кажется, что человек тебя обманывает. Постарайся держать эмоции под контролем, чтобы не терять концентрацию. Помни об осторожности даже в стрессовой ситуации. Не используй «капслок» – такие предложения считаются громким криком и могут спровоцировать человека на агрессию. Если разговор становится неприятным, закрой тему или вовсе выйди из сети и сделай себе перерыв. Еще лучше заблокировать обидчика, не

Придумай сложные пароли

Простой пароль легко запомнить и легко взломать, поэтому стоит все-таки более серьезно отнестись к его созданию. Детям необходимо придумать сложные комбинации из заглавных и строчных букв, с добавлением цифр и символов. Также для разных сайтов в интернете должны быть придуманы разные пароли, чтобы при взломе одного профиля доступ к остальным остался закрыт.

Напоследок

Не нужно делать в интернете то, что ты бы не сделал в реальной жизни. Интернет – такой же мир, в нем также действуют правила, от соблюдения которых зависит твоя безопасность. Если ты столкнулся с любым неприятным и неприемлемым поступком, сообщи об этом родителям. Мошенникам и злоумышленникам тяжело противостоять в одиночку, не бойся просить поддержки у близких людей.