10 правил безопасности в интернете

В интернете, как и в реальности, можно столкнуться с обманом, травлей и насилием. Поэтому дети должны соблюдать такие же правила безопасности, как и в реальном мире. Ниже привели рекомендации, с которыми нужно ознакомиться каждому ребенку.

Не делись своими личными данными

Одно из самых главных правил – никогда не рассказывать в сети информацию, которая помогла бы незнакомцу найти ребенка в реальности и поставить под вопрос его безопасность. Даже если кажется, что человек, с которым происходит онлайн-общение, хороший и не сделает ничего плохого, личные данные стоит оставить при себе. Речь идет о номере телефона, адресе проживания, вузе, графике работы родителей, данных из документов и даже названии спортивной команды, в которой занимается студент.

Не делись личными данными знакомых

Рассказывать в интернете о своих знакомых, друзьях и одноклассниках – плохая идея. Любые персональные данные, будь они самого молодого человека, его родителей или других людей, должны оставаться в тайне. Не стоит публиковать фотографии со своими друзьями в профиле и пересылать их в частной переписке. Перед тем как выложить совместное фото со спортивной тренировки или с праздника, сообщите об этом ребятам, изображенным на снимке.

Фильтруй информацию

Злоумышленники очень хитры – они манипулируют людьми, давят на страх и жалость, шантажируют полученными данными. Подросткам стоит понимать, что слепая вера каждому слову в интернете может привести к краже денег и личных данных, травле и преследованию. Не доверяйте всему написанному в интернете, игнорируйте подозрительные письма и сообщения от незнакомцев, не переходите по ссылкам, обещающим бесплатные подарки, тщательно обдумывайте каждое нажатие.

Если кто-то из друзей или знакомых просит в сообщении помощи, уточните, что произошло и перезвоните этому человеку, чтобы убедиться, что его страница не попала в руки мошенников.

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 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 тем, кому доверяете.

Придумай сложные пароли

Простой пароль легко запомнить и легко взломать, поэтому стоит все-таки более серьезно отнестись к его созданию. 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.

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.

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 отвечая оскорблениями на оскорбления.

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.

2 Правила безопасности в Интернете

Правила безопасности в Интернете

1. Нормы поведения и нравственные принципы одинаковы как в виртуальном, так и в реальном мире.

2. Незаконное копирование продуктов труда других людей (музыки, игр, программ и т.д.) считается плагиатом (умышленное присвоение авторства чужого произведения).

3. Не верьте всему, что в видите или читаете в интернете. При наличии сомнений в правдивости какой-то информации следует обратиться за советом.

4. Нельзя сообщать другим пользователям интернета свою личную информацию (адрес, номер телефона, любимые места для игр и т.д.).

5. Если вы общаетесь в чатах, пользуетесь программами мгновенной передачи сообщений, играете в сетевые игры, занимаетесь в интернете чем-то, что требует указания идентификационного имени пользователя.

6. Интернет-друзья могут на самом деле быть не теми, за кого они себя выдают, поэтому вы не должны встречаться с интернет-друзьями лично.

7. Нельзя открывать файлы, присланные от неизвестных вам людей. Эти файлы могут содержать вирусы или фото/видео с нежелательным содержанием.

8. Научитесь доверять интуиции. Если что-нибудь в интернете будет вызывать у вас психологический дискомфорт, поделитесь своими впечатлениями с взрослыми.

Вы должны это знать:

1. **Нежелательно размещать персональную информацию в интернете**.

2. Персональная информация — это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и личные фотографии.

3. Если вы публикуете фото или видео в интернете — каждый может посмотреть их.

4. Не отвечайте на спам (нежелательную электронную почту).

5. Не открывайте файлы, которые прислали неизвестные Вам люди. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.

6. Не добавляйте незнакомых людей в свой контакт лист в IM (ICQ, MSN messenger и т.д.)

7. Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.