

ЗА БЕЗОПАСНЫЙ ИНТЕРНЕТ! *(в рамках проведения декады «За БЕЗОПАСНЫЙ интернет»)*

10 правил безопасности в интернете для детей

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.

Спроси совета у взрослого

В любой спорной ситуации лучше советоваться с родителями. Если ребенок собирается пройти регистрацию на сайте, опубликовать свои фотографии и поделиться личной информацией, сначала желательно сообщить об этом взрослым. Родители проанализируют ситуацию и определят, насколько опасен сайт, можно ли загружать туда фотографии и какие именно снимки подходят для публикации.

Подростки, столкнувшиеся с травлей и преследованием в сети, не должны бояться рассказать об этом. О любом случае, вызвавшем смущение или тревогу, следует сообщать взрослым.

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, номере школы и класса, графике работы родителей, данных из документов и даже названии спортивной команды, в которой занимается ребенок.

Не делись личными данными знакомых

Рассказывать в интернете о своих знакомых, друзьях и одноклассниках – плохая идея. Любые персональные данные, будь они самого ребенка, 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 детям, изображенным на снимке, а они, в свою очередь, пусть посоветуются с родителями, можно ли публиковать снимок в сети.

Фильтруй информацию

Злоумышленники очень хитры – они манипулируют людьми, давят на страх и жалость, шантажируют полученными данными. Детям 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 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.

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.

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 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 несовершеннолетних в Интернете

Правила безопасности школьников в Интернете

(памятка для детей и подростков)

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 видите или читаете в интернете. При наличии сомнений в правдивости какой-то информации следует обратиться за советом к взрослым.
4. Нельзя сообщать другим пользователям интернета свою личную информацию (адрес, номер телефона, номер школы, 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, тогда выберите это имя вместе со взрослыми, чтобы убедиться, что оно не содержит никакой личной информации.
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.

Основные правила для школьников младших классов

Вы должны это знать:

1. Всегда спрашивайте родителей о незнакомых вещах в интернете. Они расскажут, что безопасно делать, а что нет.
2. Прежде чем начать дружить с кем-то в интернете, спросите у родителей как безопасно общаться.
3. Никогда не рассказывайте о себе незнакомым людям. Где вы живете, в какой школе учитесь, номер телефона должны знать только ваши друзья и семья.
4. Не отправляйте фотографии людям, которых вы не знаете. Не надо чтобы незнакомые люди видели ваши личные фотографии.
5. Не встречайтесь без родителей с людьми из интернета вживую. В интернете многие люди рассказывают о себе неправду.
6. Общаясь в интернете, будьте дружелюбны с другими. Не пишите грубых слов, читать грубости так же неприятно, как и слышать. Вы можете нечаянно обидеть человека.
7. Если вас кто-то расстроил или обидел, обязательно расскажите родителям.

Основные правила для школьников средних классов

Вы должны это знать:

1. При регистрации на сайтах старайтесь не указывать личную информацию, т.к. она может быть доступна незнакомым людям. Также не рекомендуется размещать свою фотографию, давая тем самым представление о том, как вы выглядите посторонним людям.
2. Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть вас во время разговора, т.к. он может быть записан.
3. Нежелательные письма от незнакомых людей называются «спам». Если вы получили такое письмо, не отвечайте на него. В случае, если вы ответите на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылать вам спам.
4. Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.
5. Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя в вашем отношении неподобающим образом, размещает, либо угрожает разместить видео и фото, компрометирующее вас (либо

с вашим участием) в сети интернет, сообщите об этом родителям, либо лицу, которому вы доверяете.

6. Если вас кто-то расстроил или обидел, расскажите все взрослому, которому вы доверяете.

Основные правила для школьников старших классов

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.

8. Если рядом с вами нет родственников, не встречайтесь в реальной жизни с людьми, с которыми вы познакомились в интернете. Если ваш виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к вашей заботе о собственной безопасности!

9. Никогда не поздно рассказать взрослым, если вас кто-то обидел.

Правила безопасности при посещении сайтов

и по приему электронной почты

1. Не ходите на незнакомые сайты.

2. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на макровирусы.

3. Если пришел exe-файл, даже от знакомого, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину в вашей программе чтения почты.

4. Не заходите на сайты, где предлагают бесплатный Интернет (не бесплатный e-mail, это разные вещи).

5. Никогда никому не посылайте свой пароль.

6. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.