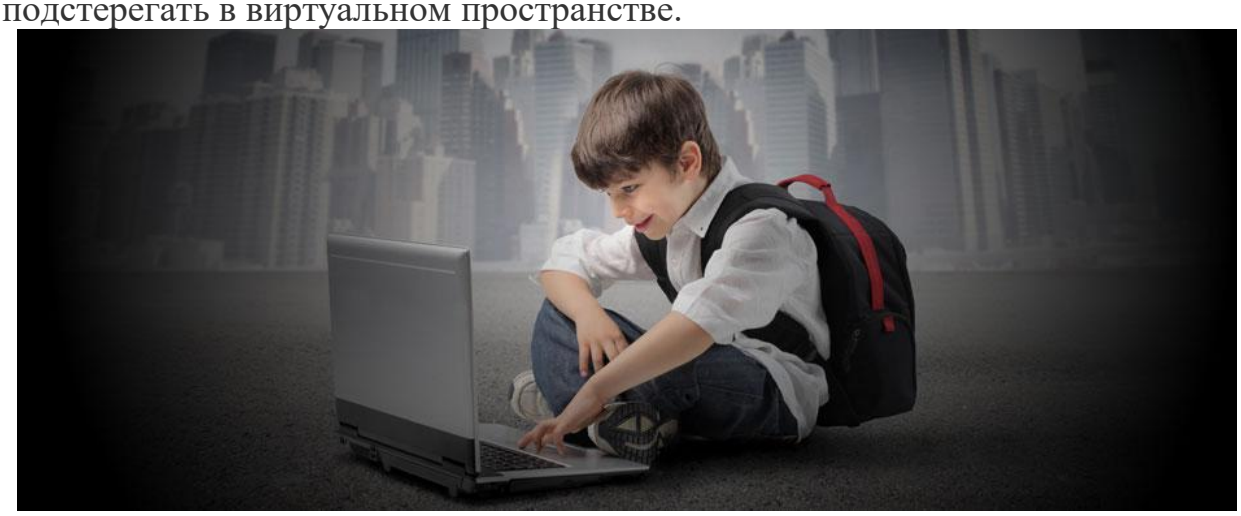
Правила безопасного поведения в сети Интернет

Всегда ли безопасно пользоваться Интернет-сетью? Эксперты в один голос утверждают, что в этом смысле виртуальный мир ничем не отличается от реального: там тоже есть сверстники, которые устраивают травлю, плохие компании, маньяки и мошенники. Разница только в том, что происходящее на улице родители могут хорошо себе представить, а вот ловушки, в которые можно угодить в Интернете, многие пока еще не изучили до конца.

Данные правила по безопасному поведению помогут родителям, учителям и школьникам избежать различных опасностей, которые могут подстерегать в виртуальном пространстве.



Правило 1. Храните тайны.

В информационном пространстве нам часто приходится вводить свои данные: ФИО, адрес, дату рождения, номера документов. Безопасно ли это?

Персональные данные (имя, фамилия, адрес, дата рождения, номера документов) можно вводить только на государственных сайтах или на сайтах покупки билетов. И только в том случае, если соединение устанавливается по протоколу https. Слева от адреса сайта должен появиться значок в виде зеленого замка — это означает, что соединение защищено.

Правило 2. Будьте анонимны.

Создавая свой профиль в социальных сетях, нужно максимально избегать привязки к «физическому» миру. Нельзя указывать свой адрес, дату рождения, школу, класс. Лучше использовать очевидный псевдоним.

Не рекомендуется ставить свою фотографию на аватар, если вам не исполнилось хотя бы 15-16 лет. Все дети и подростки младше этого возраста, публикуя свои фотографии, рискуют стать жертвой злоумышленника.

Правило 3. Не общайтесь с незнакомцами.

Есть несколько главных опасностей, с которыми можно столкнуться в Интернете. По большому счету, они мало чем отличаются от тех, что угрожают нам в реальной жизни.

Злоумышленники здесь просто используют другие средства.

Буллинг. Ребенка обзывают или травят в Интернете, чаще всего без какой-либо причины. К жертве могут прицепиться из-за фотографии в профиле или из-за поста в социальных сетях.

Педофилы. Просят прислать личные фотографии, а при отказе угрожают расправой над членами семьи или шантажируют другими способами.

Мошенники. Пытаются завладеть данными пользователя или втянуть ребенка в опасную финансовую авантюру.

Главное средство защиты от всех этих угроз — конфиденциальность. Нельзя выкладывать свои фотографии в Сеть. Следует ограничить доступ к информации о всех сторонах своей жизни, будь то онлайн или офлайн.

Сообщать личные данные можно только проверенным людям. Тех, кто пытается вас как-то задеть и обидеть (так называемых троллей), нужно просто игнорировать.

Правило 4. Учитесь распознавать злоумышленников.

На что необходимо обратить внимание, прежде чем вступить в диалог? Что сигнализирует об опасности?

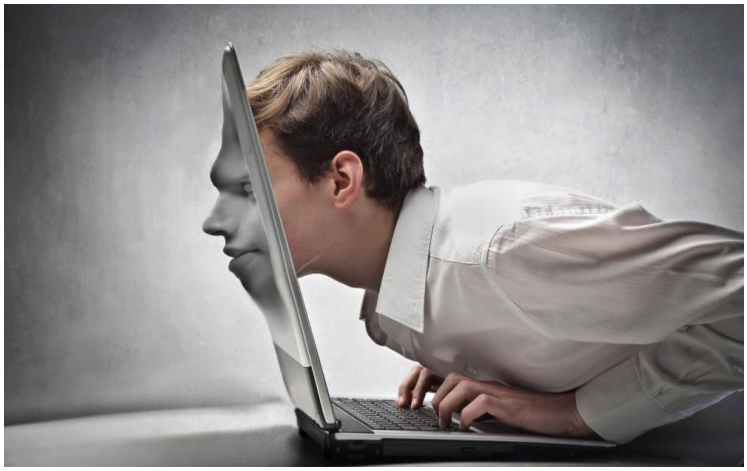
- Вы не знакомы с этим человеком в реальной жизни.
- Ваш собеседник явно старше вас.
- У него нет или очень мало друзей в социальной сети.
- Собеседник о чем-то вас просит: сфотографироваться, прислать какие-либо данные и т.д.

Правило 5. Храните фото- и видеоматериалы в недоступном месте.

Правила публикации собственных фотографий очень простые. Если вы не хотите, чтобы они стали достоянием общественности, то просто не выкладывайте их в Интернет и никому с его помощью не отправляйте. Даже мессенджеры «умеют» копировать переписку в «облако», так что вы можете потерять контроль над своими снимками.

Если что-то куда-то было отправлено или где-то опубликовано - это ушло в Сеть. Важно помнить, что ни в коем случае нельзя выкладывать фотографии документов, будь то своих или чужих.

Правило 6. Будьте бдительны.



Плохая новость — удалить ничего не получится. Все, что однажды попало в Сеть или даже в смартфон, останется там навсегда. Как правило, стереть данные из Сети невозможно.

Единственный способ избежать утечки информации — не делиться ею.

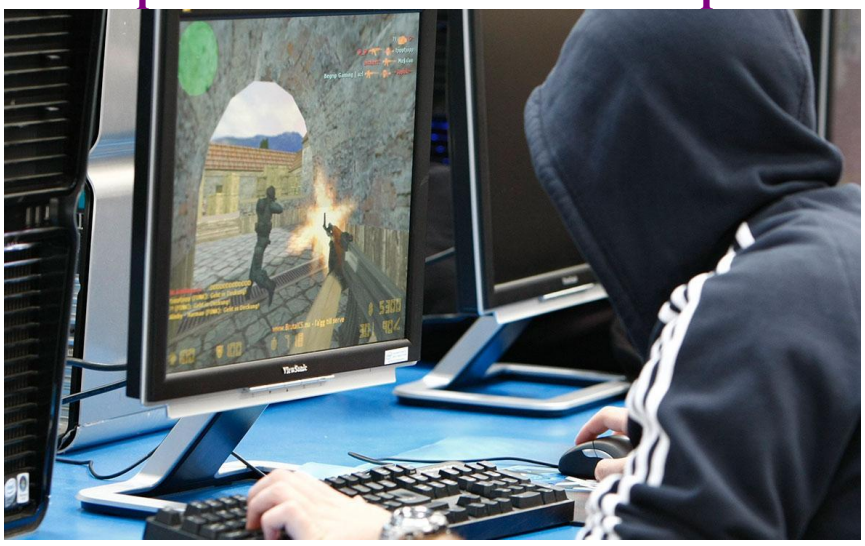
Правило 7. Не сообщайте свое местоположение.

Данные геолокации позволяют всему миру узнать, где вы живете и учитесь, где проводите свободное время, в каких акциях участвуете, какие шоу и спектакли любите, как отдыхаете. Отследить местоположение человека теперь не составляет труда.

Для ребенка это может представлять большую опасность. Но полностью отключить геолокацию на детском телефоне нельзя. Родителям полезно использовать специальные программы, чтобы знать, где находится их ребенок.

Чтобы сделать геолокацию максимально безопасной, нужно следить за тем, чтобы местоположение не отображалось на «искабельных» объектах — особенно на фотографиях. На телефонах, в настройках камеры, как правило, можно запретить геометки.

Правило 8. Внимание – на игры.



Не только мессенджеры и социальные сети могут представлять опасность для детей. Многие угрозы могут также исходить и от онлайн-игр.

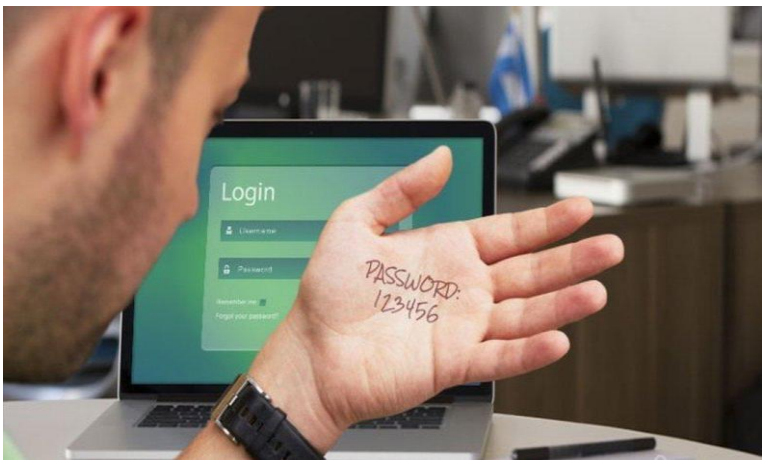
Там ребенок даже более уязвим, поскольку им проще манипулировать: игровые объекты, членство в командах, внутриигровые социальные связи — все это может стать механизмом манипуляции для мошенников, педофилов или даже вербовщиков различных экстремистских группировок. Вот почему в игре нужно вести себя особенно внимательно.

Правило 9. Учитесь замечать поддельные сайты.

Фишинг — это способ выманивать у человека его данные: логин, название учетной записи и пароль.

Происходит это так: пользователю присылают ссылку на сайт, очень похожую на настоящий адрес почтового сервиса или социальной сети. Как правило, фишеры специально покупают такие домены. Например, для mail.ru это может быть «meil.ru», а для vk.com — «vk-com.com». Злоумышленник ждет, когда человек введет логин или пароль на поддельном сайте. Так он узнает данные, а потом использует их для входа в настоящий профиль своей жертвы.

Правило 10. Тренируйте память.



Можно ли пользоваться сервисами, которые сохраняют пароли? Если в профиле содержится действительно важная информация, то, увы, нет. Почему?

Это удобно, но онлайн-сервисы для хранения паролей ненадежны. Их часто

взламывают и копируют оттуда пароли пользователей. Чаще всего жертвы узнают об этом лишь спустя какое-то время, если вообще узнают. Нередко такие сайты и сервисы создаются мошенниками специально для того, чтобы собирать пароли.

Пароли должны быть уникальными. Цифры и спецсимволы значительно усложняют процесс подбора. В соцсети, мессенджеры и почту безопаснее входить через приложения, а вот в браузерах ввода паролей следует избегать. Все приложения должны устанавливаться родителями или под их контролем.

Правило 11. Будьте аккуратнее с Интернет-покупками.

Совершая покупки в Интернет-магазинах, сохраняйте здоровый скептицизм. Помните: цена не может быть слишком низкой, тем более, если вы рассчитываете приобрести оригинальную продукцию бренда. Изучите историю магазина в сети, проверьте наличие контактов, выясните, можно ли туда приехать и познакомиться вживую. Обратите внимание на отзывы. Они не должны быть «будто под копирку». А вообще, все платежи должны согласовываться с родителями и происходить только под их присмотром.

Все сервисы, которые принимают деньги, должны иметь зеленый значок «https» рядом с названием. Если такого значка нет, лучше не пользоваться страницей. Впрочем, даже его наличие стопроцентной гарантии не дает.

Часто в пабликах «ВКонтакте» предлагают что-то купить с использованием платежной системы Qiwi. Тут тоже нужно проявлять бдительность и внимательно изучать отзывы о продавце. В соцсетях есть немало мошенников, которые после получения денег удаляют страницы и исчезают.

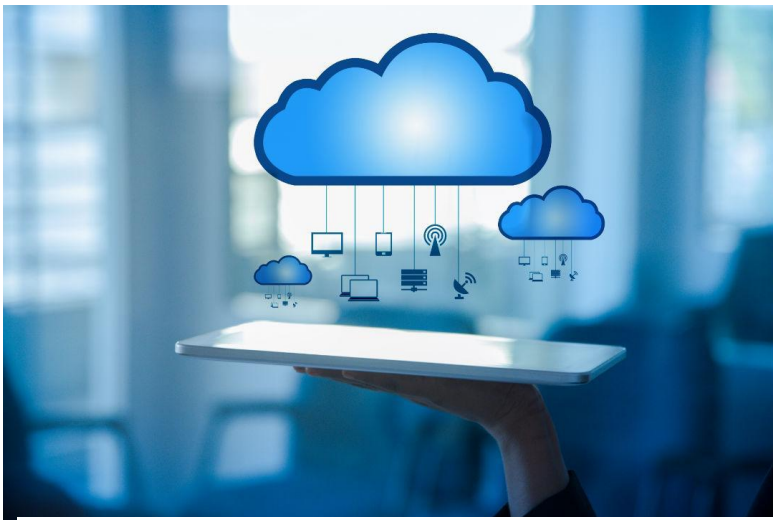
Правило 12. Проверяйте информацию.

Проверка информации в Интернете — довольно сложный и трудоемкий процесс. Даже взрослые не всегда могут эффективно справиться с ним. Однако есть несколько формальных признаков того, что вы попали на «желтый» сайт, которому не стоит верить безоговорочно. Это, как правило, кричащие заголовки, назойливо всплывающие окна, обилие рекламы. Чтобы проверить информацию, которую вы получили в Интернете, следуйте следующим рекомендациям:

- поищите еще два-три источника, желательно и на других языках тоже;
- найдите первоисточник и задайте себе вопрос: «Можно ли ему доверять?»;
- проверьте, есть ли в Сети другие мнения и факты, которые опровергают или подтверждают сказанное.

Если нужно узнать какой-то факт или выяснить, что значит непонятный термин, можно обратиться к «Википедии». Там редко можно встретить неверную информацию, но слепо доверять открытой цифровой энциклопедии тоже не стоит.

Правило 13. Позаботьтесь об «облаке».



Насколько надежны хранилища, вроде «Облако» Mail.Ru, и можно ли там без опаски хранить документы?

Специалисты говорят, что облачное хранилище можно обезопасить, если предварительно зашифровать документы с помощью PGP или использовать программу для создания архива, поместив в него отсканированные документы.

При создании архива нужно указать опцию «непрерывный архив» (solid archive) и поставить на этот архив хороший пароль. Например,такой:«kn23iuhuio12njkpuiy89y7&R&TFTGIY* (UYT&*T^G!*OUH*&GYUIHJK)».

Или хотя бы такой:«во#полеберезастояла123». Не рекомендуется использовать один и тот же пароль для разных архивов.

Правило 14. Соблюдайте сетевой этикет.

Человечество только учится общаться в Сети, но правила хорошего тона здесь ничем не отличаются от тех, которые нужно соблюдать в реальном мире. Не оскорбляйте других, не будьте навязчивы, не позволяйте

своим негативным эмоциям выходить из-под контроля, пишите грамотно.

Правило 15. Главный секрет безопасности в сети.

Не нужно делать в Интернете ничего того, чего бы вы не стали делать в физическом мире. Разница между виртуальной и реальной действительностью минимальна.

Что касается родительского поведения, то в Сети оно тоже не должно отличаться от поведения «в офлайне». От ребенка нельзя добиться повиновения путем запретов и жесткого контроля. Однако и ощущения вседозволенности в Интернете тоже быть не должно.