15 ПРАВИЛ
БЕЗОПАСНОГО ПОВЕДЕНИЯ В ИНТЕРНЕТЕ

Всегда ли для ребенка безопасно пользоваться Сетью?

Эксперты утверждают, что в этом смысле виртуальный мир не отличается от реального: там тоже есть сверстники, которые устраивают травлю, плохие компании, маньяки и мошенники. Маленьких детей не отпускают на улицу одних, а у подростков всегда узнают, где они, с кем, чем занимаются и когда будут дома. Такой же уровень заботы нужен и в Сети. Разница только в том, что происходящее на улице родители хорошо себе представляют, а вот ловушки, в которые можно попасть в интернете, многие пока еще не изучили до конца. И все же ребенка нельзя держать взаперти, не выпуская ни за порог, ни в Сеть.
Данные правила по безопасному поведению в интернете составлены экспертами по кибербезопасности корпорации Mail.Ru Group и порталом «Учеба.ру». Они помогут родителям, учителям и детям избежать различных опасностей виртуального пространства, которые окружают каждого современного ребенка и взрослого во Всемирной сети.

№ 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.

Вряд ли ребенку потребуется регистрация на государственных сайтах, но даже если она нужна, делать это в любом случае надо под руководством родителей. Важно помнить, что ни в коем случае нельзя передавать через Сеть данные любых документов и банковских карт. Даже (и тем более) если кто-то об этом просит, старается убедить в том, что возникла критическая ситуация, торопит и повторяет, что нужно срочно прислать информацию.

Если такая ситуация возникла, ребенку нужно сразу связаться с родителями. Если ему говорят, что никому ничего сообщать нельзя, и пугают неприятными последствиями, тем более следует срочно обо всем рассказать семье. Запугивание и попытки во что бы то ни стало получить сведения говорят о том, что перед вами мошенники.

№ 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: по нему должно быть ясно, что это не настоящее имя (ведь использовать ложные данные: «Алексей» вместо «Александр» — по правилам соцсетей запрещено).

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

№ 3 НЕ РАЗГОВАРИВАЙТЕ С НЕЗНАКОМЦАМИ

Есть несколько главных опасностей, с которыми можно столкнуться в интернете. По большому счету они мало 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, «потому что так весело». К жертве могут прицепиться из-за фотографии в профиле или из-за поста в соцсетях.

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 их можно только проверенным людям: родным, близким и людям, которые знакомы вам лично, а не через интернет.

Тех, кто пытается вас как-то задеть и обидеть (так называемых троллей), нужно просто игнорировать.

№ 4 РАСПОЗНАЙТЕ ЗЛОУМЫШЛЕННИКА

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

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

№ 5 ХРАНИТЕ ФОТО В НЕДОСТУПНОМ МЕСТЕ

Правила публикации собственных фотографий очень простые — если вы не хотите, чтобы они стали достоянием общественности, нельзя выкладывать их в интернет и отправлять кому-то с его помощью. Вообще. 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 — своих или чужих. А фото других людей стоит выкладывать только в случае, если они на это согласны.

№ 6 БУДЬТЕ БДИТЕЛЬНЫ

Плохая новость — удалить ничего не получится.

Все, что 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.

№ 7 НЕ СООБЩАЙТЕ СВОЕ МЕСТОПОЛОЖЕНИЕ

Данные геолокации позволяют всему миру узнать, где вы живете и учитесь, 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 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.

№ 8 ВНИМАНИЕ — НА ИГРЫ

Правила безопасности есть не только в соцсетях и мессенджерах. Все основные угрозы могут 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.

№ 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.

№ 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.

№ 11 АККУРАТНЕЕ С ПОКУПКАМИ

Главное правило интернет-покупок такое: доступ ребенка к деньгам должен быть ограниченным и находиться под контролем родителей.

Основные финансовые потери обычно происходят через телефон. Необходимо подключить услуги блокировки платного контента, не класть много денег на счет детского телефона и контролировать расходы. Все остальные 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 исчезают.

№ 12 ПРОВЕРЯЙТЕ ИНФОРМАЦИЮ

Проверка информации — довольно сложный процесс, и даже взрослые люди далеко не всегда справляются с этим. Есть несколько формальных признаков того, что вы попали на «желтый» сайт, которому не стоит

верить безоговорочно. Это кричащие заголовки, обилие рекламы или если читателя, который кликнул на новость, перекидывают куда-то дальше.

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 совсем уж откровенную чепуху, но слепо доверять открытой цифровой энциклопедии не стоит: даже в ней попадаются ошибки.

№ 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.

№ 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 навязчивым, не позволяйте своим негативным эмоциям выходить из-под контроля, пишите грамотно.

Как и в жизни, в Сети нам приходится бывать в разных сообществах, и правила общения могут различаться. Вежливый человек, попав в незнакомое общество, прежде всего попытается узнать его особенности. Где-то принято общаться на «вы», а где-то — на «ты», где-то смайлики уместны, а где-то — нет. Есть компании, где приветствуется использование сетевого сленга, а есть такие, где его просто не поймут или посчитают вас безграмотным.

Впрочем, существуют правила, актуальные для любых сообществ:

- не привлекайте к себе внимание за счет эпатажа;
- не отходите от темы разговора: «флуд» считается одним из главных «грехов» в Сети;
- не игнорируйте вопросы собеседника, кроме явного троллинга или оскорблений — подобную беседу нужно немедленно прекратить;
- никогда не участвуйте в травле: буллинг в Сети ничем не отличается от реального и одинаково опасен и для жертвы, и для агрессора.

№ 15 ГЛАВНЫЙ СЕКРЕТ БЕЗОПАСНОСТИ В СЕТИ

Не нужно делать в интернете ничего, что бы вы не стали бы 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. Вместе учитесь вести безопасный образ жизни, как реальной, так и виртуальной.