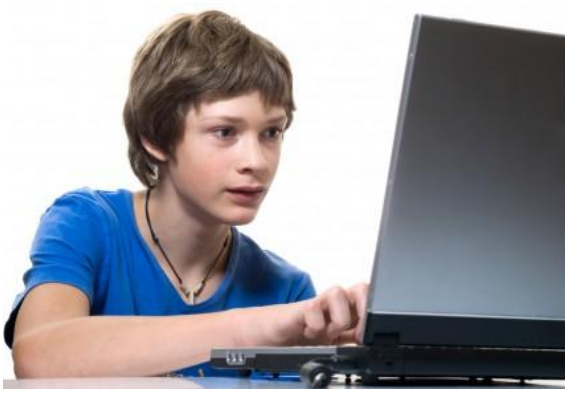
Как сделать пребывание в сети для ребенка безопасным?

По материалам сайта paidagogos.com

Уважаемые родители! Сегодня сложно себе представить ребёнка, который не является активным пользователем интернета. Год за годом мы наблюдаем, как российские интернет-пользователи становятся моложе. Дети нашего времени развиваются в мире, который намного отличается от мира, в котором выросли их папа и мама. Одним из главнейших факторов развития современного ребёнка становится среда информационных технологий, где интернет занимает ведущее место.

Однако наряду со всеми преимуществами информатизации нашего мира, интернет несёт в себе немалую опасность для подрастающего поколения. И маленькие дети, и подростки не могут сполна оценить все риски, с которыми они сталкиваются при вхождении в онлайн-среду. С помощью наших советов, разъяснений и рекомендаций вы сделаете пребывание вашего ребёнка во всемирной паутине безопасным и полезным.

Интернет-риски



Вспомните случаи, когда ваш ребёнок «сидит в интернете». Наверняка ли вы знаете, чем он занимается, с кем он общается?

Одно из исследований показало, что, хоть и многие папы и мамы предоставляли детям информацию о необходимости безопасно пользоваться интернетом и рассказывали о правилах такого пользования, всё же меньшая часть родителей отслеживает занятия детей в интернете. Большинство детей заявило, что они не спрашивают разрешения родителей о пользовании интернетом, а также поводят время в сети без ограничений.

Часто родители думают, что интернет не несёт никакой опасности детям. Компьютер родители воспринимают как новое современное средство обучения. Они считают, что если ребёнок дома, то нет никакой надобности беспокоится о них. Однако не во всех случаях это так. Родителям необходимо быть в курсе дел своего ребёнка в интернете — наравне с интересом к другим сферам его деятельности.

Опасности в интернете

- вредоносные программы
- кибермошенничество
- социальные сети
- блоги
- содержание контента
- интернет-зависимость

Вредоносные программы

Вредоносные программы — это разнообразное программное обеспечение, умышленно созданное для нанесения вреда электронным устройствам или похищения информационных ресурсов, данных. Это вирусы, «троянские кони», «черви», «боты», программы слежки и. т. д. Вредоносные программы, попадая на компьютер, способствуют снижению скорости при обмене данными, а также используют ваш компьютер как базу для распространения своих вредоносных данных. Они могут использовать ваш e-mail или профиль социальной сети как разносчика спама («мусора»). Такие опасные файлы могут попадать на ваш компьютер следующим путём:

- посредством посещения сомнительных веб-сайтов и скачанных с них файлов;
- из электронной почты через полученный спам;
- при помощи электронных носителей (CD, флешек).

Помогите ребёнку предупредить появление опасных программ на компьютере.

Установите антивирусник**.** Антивирусные программы помогут уберечь ваш компьютер от сомнительных файлов, а специальные почтовые фильтры предотвратят попадание спама на электронную почту. Такие программы останавливают вредоносные атаки.

Устанавливайте надёжные программы**.** Объясните ребёнку, что лицензионное программное обеспечение или программы из проверенных источников не наносят вреда компьютеру, в отличие от установки «пиратских» программ.

Не открывайте приложенные файлы**.** Научите ребёнка не открывать вложения, присланные с неизвестных адресов электронной почты: они нередко бывают вирусами.

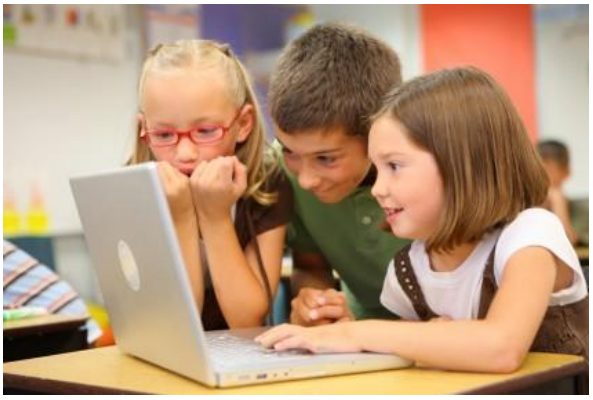
Обновляйте антивирус. А лучше установите автообновление.

Проверяйте компьютер на наличие вирусов. Сканируйте чаще, не реже раза в неделю.

Резервируйте. Научите детей делать дополнительные копии нужных файлов.

Обратите внимание на пароли. Учите детей создавать сложные уникальные пароли к входу в электронный почтовый ящик или социальную сеть, а также периодически менять их. Расскажите, что пароль не нужно никому сообщать. Если же он стал известен — нужно поменять.

Чужие устройства. Расскажите ребёнку, что если он использовал чужой компьютер (планшет, смартфон) для просмотра своей странички в социальной сети, то должен обязательно выходить из аккаунта по окончанию работы. Нельзя на чужих устройствах сохранять пароли — это могут использовать злоумышленники.



Кибермошенничество

Одним из опасных видов преступлений является кибермошенничество — хищение личной важной информации интернет-пользователя: пароли, коды, данные паспорта и банковских карт и т. д. Смс, отправленное для подтверждения скачивания интересной игры, песни, программы, мелодии звонка, книги, может стать причиной снятия с телефона немалой суммы. Это можно заметить, если вы только выделили средства для пополнения счёта телефонного номера вашего ребёнка, а он тут же подходит с сообщением, что денег на разговоры уже не осталось.

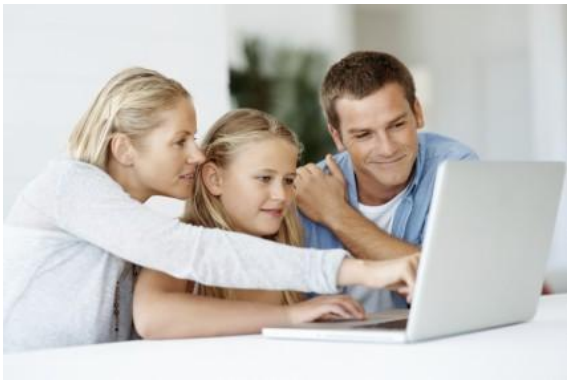
В таком случае, нужно ребёнка научить быть осторожным с кибермошенничеством.

Информируйте. Объясните ребёнку, что сегодня в сети очень много случаев мошенничества, приведите примеры. Обсуждайте вместе, стоит ли пользоваться теми или иными услугами в сети, особенно если они платные.

Разберите ситуацию. Если инцидент произошёл, выясните у ребёнка, какой сайт он посещал, куда он нажимал, что хотел, какие сообщения читал и т.д. Постарайтесь восстановить всю цепочку действий ребёнка, всё сохраните: это может пригодиться.

Следите за банковскими картами. Ребёнок не должен иметь свободный доступ к платёжным картам родителей: так он не сможет самостоятельно совершать покупки в интернете.

Проверьте надёжность. Если вы с ребёнком решили приобрести товар или услугу, то убедитесь в безопасности выбранного ресурса (интернет-магазина): проверьте наличие реквизитов, почитайте правила и отзывы.



Социальные сети

Дети сегодня пользуются как социальными сетями, предназначенными для детей, так и предназначенными для взрослых (Вконтакте, Одноклассники, Facebook, YouTube, Twitter). Заведя аккаунт в соцсети, дети могут общаться как с одноклассниками и близкими друзьями, так и с людьми, проживающими в разных странах.

Регистрируясь в социальной сети, ребёнок должен понимать, что его действия на своей страничке могут просматриваться различными пользователями.

Доступная информация является уязвимой. Каким образом? Например, появлением кибербуллинга или груминга.

Кибербуллинг представляет собой появление сообщений в социальных сетях, содержащих угрозы, оскорбления, запугивание или травлю. Есть

случаи, когда чью-то страницу могут взломать, разместив на ней негативный контент, унижающий и оскорбляющий человека.

Вероятность встреч с незнакомыми людьми и **грумминг** — ещё одна опасность использования социальных сетей. Добавляя в друзья совершенно незнакомых людей и общаясь с ними, ребёнок подвергает себя опасности. Наивный малыш может разгласить информацию о себе и своей семье, подвергнуться давлению, вымогательству и шантажу. Нередки случаи, когда, представляясь сверстником в онлайн-чате, злоумышленник настаивает на личной встрече, которая может обернуться для ребёнка насилием или даже похищением.

Родителям следует просвещать ребёнка по безопасному использованию сайтов социальных сетей.

Интересуйтесь виртуальными друзьями ребёнка**.** Узнайте, нет ли среди его «друзей» сомнительных личностей, которые причиняют беспокойство ребёнку. Не паникуйте. Скажите ребёнку, что о таком необходимо рассказывать, и что родители помогут справиться с появившейся проблемой.

Создайте правила**.** Как только ваши дети станут самостоятельными при пользовании интернетом, объясните их несложные правила: можно ли им заводить аккаунты с социальных сетях, кого они в таком случаем могут принимать в друзья, сколько времени им уделять на такое виртуальное общение и т. д. В случае несоблюдения правил — удалите страницу из сети самостоятельно или обратившись к администратору.

Обращайте внимание на возраст**.** Обратите внимание на то, что большая часть социальных сетей не допускает участия в них детей, не достигших 13-14-летнего возраста.

Следите за контентом**.** Каждая социальная сеть имеет правила пользования и ограничения относительно содержания публикаций. Обычно, это контент оскорбительного характера и т. п. Ознакомьтесь с ребёнком с этими правила и следите, чтобы юный пользователь интернета их не нарушал. Возьмите в привычку время от времени просматривать страничку вашего ребёнка.

Запрет на встречи**.** Запретите ребёнку лично встречаться с кем-то, с кем они познакомились в сети. Объясните реальную угрозу таких встреч. А лучше — взять за правило не принимать незнакомцев в друзья. Пусть дети общаются в виртуальном мире с реально знакомыми людьми.

Лучше псевдоним. Расскажите ребёнку, что в целях безопасности лучше не разглашать настоящее имя и фамилия, а придумать псевдоним.

Отслеживайте группы. Смотрите, в какие сообщества и группы присоединяется ваш ребёнок, и какого рода информация там проходит.

Следите за фото. Нередко фотографии, которые выкладывает ребёнок в интернет, могут стать источником дополнительной информации о вашей семье. Попросите ребёнка не публиковать фото, из которого можно почерпнуть такую информацию.

Сдерживаем эмоции. Следите, чтобы ребёнок не был слишком эмоционален в социальных сетях. Злоумышленники обращают внимание именно на эмоционально неустойчивых детей.

Интернет-угрозы. Поддерживая доверительные отношения с ребёнком, узнавайте от него, не поступают ли в социальных сетях в его адрес угрозы или сообщения оскорбительного характера. При наличии таковых, вовремя примите меры.

Блоги

Ведение блогов, иными словами «сетевых дневников», очень популярно среди подростков. Многие из них ведут блоги втайне родителей. Если же ваш ребёнок является автором блога, то необходимо проследить, чтобы юный автор не слишком много выкладывал в сеть информации личного характера о себе и семье.

Избежать проблем поможет следование рекомендациям:

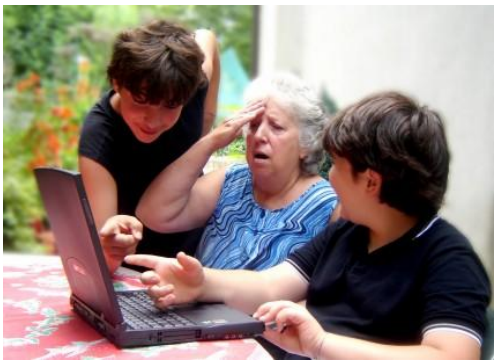
Предварительный просмотр. Родителям следует предварительно посмотреть содержание того, что собирается публиковать в блоге ваш сын или дочь, и только после этого одобрять или нет публикацию.

Адекватна ли информация? Если да, то право на жизнь у такой статьи (фотоподборки) есть.

Проверяем блог. Время от времени знакомьтесь с содержанием блога ребёнка, читайте комментарии.

Мониторим. Сделайте подборку лучших блогов и продемонстрируйте ребёнку хороший вариант при возникновении какой-то проблемы.

Контент



Что такое «контентные риски»? Это присутствие в интернете материалов противозаконного, неэтичного и иного вредоносного характера. Такие материалы могут быть представлены текстами, изображениями, звуковыми и видеофайлами, ссылками и баннерами на посторонние сайты и т.д. Сегодня вся всемирная сеть – это рискованное пространство. Несовершеннолетний гражданин может столкнуться с порнографическим контентом, призывами использованию и приобретению наркотиков, призывами к участию в экстремистских действиях. Такой контент может нанести психологический вред сознанию детей и подростков, изменить их ценностные ориентации. Особенно опасными считаются сайты, где представлены способы причинения вреда людям, боли, методы похудения, самоубийства, применения наркотических веществ, сайты человеконенавистнических и экстремистских организаций, порнографические сайты.

Чтобы предупредить влияние контентных рисков, родителям следует обращать внимание на следующее:

Ограничиваем доступ. Сегодня есть программное обеспечение, ограничивающее доступ несовершеннолетней аудитории к сомнительному контенту. Воспользуйтесь соответствующими функциями вашей антивирусной программы или установите программу родительского контроля. В поисковых системах активируйте функцию безопасного поиска.

Следим за активностью в сети. Просмотр истории посещения сайтов и поисковых запросов позволит оставаться уверенным в безопасности контента.

Объясняем. Беседуйте с детьми на предмет того, что далеко не всё, что находится в интернете, — правда, добродетель и польза. Учите их самостоятельно фильтровать информацию, увиденную в интернете.

Интернет-зависимость

Актуальной проблемой является интернет-зависимость, которая представляет собой острое желание войти в интернет во время его отсутствия. Такое состояние негативно действует на организм, хотя и не разрушает его прямым способом. Интернет-зависимость схожа с зависимостью от азартных игр. Она также характеризуется потерей ощущения времени, неумением вовремя остановиться, отрывом от реальности, раздражительностью и отчаянием по причине отсутствия возможности выхода в интернет.

Полезно знать. Более 90% интернет-зависимых пользователей используют сервисы, связанные с общением.

Как быть, если вы заметили у ребёнка такие симптомы?

Наладьте контакт. Узнайте, что ребёнку интересно и что его беспокоит.

Не запрещайте интернет. Но установите нормы использования.

Один компьютер. Пусть к интернету будет подключен один компьютер – так легче будет отследить деятельность ребёнка в сети. В других устройствах интернет необходимо убрать.

Учите ребёнка управлению временем. Так он осознает вред бездумной траты времени в интернете.

Альтернатива. Предложите ребёнку интересное занятие, и тогда у него не будет времени на времяпрепровождение у компьютера / планшета / смартфона.

Обсуждайте. Поговорите с ребёнком на тему, почему он не может обходиться без интернета. Дайте понять, что ничего не случится, ели он на какое –то время покинет сеть.

Совет психолога. Тяжёлые случаи требуют консультации специалиста.

Следуйте нашим советам – так вы сможете сделать пребывание ваших детей в интернете безопасным и научите их медиаграмотности.