Правила безопасности детей в интернете

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?

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:

1. **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.
2. **Устанавливайте надёжные программы.** Объясните ребёнку, что лицензионное программное обеспечение или программы из проверенных источников не наносят вреда компьютеру, в отличие от установки «пиратских» программ.
3. **Не открывайте приложенные файлы.** Научите ребёнка не открывать вложения, присланные с неизвестных адресов электронной почты: они нередко бывают вирусами.
4. **Обновляйте антивирус.** А лучше установите автообновление.
5. **Проверяйте компьютер на наличие вирусов.** Сканируйте чаще, не реже раза в неделю.
6. **Резервируйте.** Научите детей делать дополнительные копии нужных файлов.

7. **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.

8. **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:

1. **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.

2. **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.

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

4. **Проверьте надёжность.** Если вы с ребёнком решили приобрести товар / 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 (Смешарики — «Шарарам»), 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:

1. **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.

2. **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.

3. **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.

4. **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.

5. **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.

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

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

8. **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.

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

10. **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:

1. **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.

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

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

4. **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:

1. **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.

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

3. **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 с 1996 года 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?

1. **Наладьте контакт.** Узнайте, что ребёнку интересно и что его беспокоит.
2. **Не запрещайте интернет.** Но установите нормы использования.
3. **Один компьютер.** Пусть к интернету будет подключен один компьютер – так легче будет отследить деятельность ребёнка в сети. В других устройствах интернет необходимо убрать.
4. **Учите ребёнка управлению временем.** Так он осознает вред бездумной траты времени в интернете.
5. **Альтернатива.** Предложите ребёнку интересное занятие, и тогда у него не будет времени на времяпрепровождение у компьютера / планшета / смартфона.
6. **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.
7. **Совет психолога.** Тяжёлые случаи требуют консультации специалиста.

Выводы

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

Как обеспечить безопасность детей в интернете

Рекомендации партнеров

Google: Мы сотрудничаем с российскими и международными организациями, которые занимаются проблемами детской безопасности в Интернете. В этом разделе представлены практические рекомендации о том, как помочь юным пользователям оставаться в безопасности в киберпространстве и избежать существующих рисков.

- Нежелательный контент
- Интернет-знакомства
- Кибербуллинг
- Кибермошенничество
- Интернет- и игровая зависимость
- Вредоносные программы
- Что делать, если ребенок все же столкнулся с какими-либо рисками
- Линия помощи “Дети Онлайн”
- Как защитить ребенка от нежелательного контента в Интернете

Контентные риски – это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д.

Как помочь ребенку избежать столкновения с нежелательным контентом:

- Приучите ребенка советоваться со взрослыми и немедленно сообщать о появлении нежелательной информации подобного рода;
- Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернете – правда. Приучите их спрашивать о том, в чем они не уверены;
- Старайтесь спрашивать ребенка об увиденном в Интернете. Зачастую, открыв один сайт, ребенок захочет познакомиться и с другими подобными ресурсами;
- Включите программы родительского контроля и безопасного поиска, которые помогут оградить ребенка от нежелательного контента;
- Постоянно объясняйте ребенку правила безопасности в Сети;

Тем не менее помните, что невозможно всегда находиться рядом с детьми и постоянно их контролировать. Доверительные отношения с детьми, открытый и доброжелательный диалог зачастую может быть гораздо конструктивнее, чем постоянное отслеживание посещаемых сайтов и блокировка всевозможного контента.

- Используйте специальные настройки безопасности (инструменты родительского контроля, настройки безопасного поиска и другое).
- Выработайте «семейные правила» использования Интернета. Ориентируясь на них, ребенок будет знать, как поступать при столкновении с негативным контентом.
- Будьте в курсе того, что ваш ребенок делает в Интернете. Чаще беседуйте с ребенком о том, что он делает в Сети.

Как научить ребенка быть осторожным при знакомстве с новыми людьми в Интернете

Общение в Интернете может повлечь за собой коммуникационные риски, такие как незаконные контакты (например, груминг), киберпреследования, кибербуллинг и др.

Даже если у большинства пользователей чат-систем (веб-чатов или IRC) добрые намерения, среди них могут быть и злоумышленники. В некоторых случаях они хотят обманом заставить детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в

Интернете и др. В других случаях они могут оказаться преступниками в поисках жертвы. Специалисты используют специальный термин «груминг», обозначающий установление дружеских отношений с ребенком с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), злоумышленник входит в доверие к ребенку, пытается узнать личную информацию и договориться о встрече.

Предупреждение груминга:

- Будьте в курсе, с кем контактирует в Интернете ваш ребенок, старайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они лично знают всех, с кем они общаются;
- Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также пересылать интернет-знакомым свои фотографии;
- Если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу;
- Не позволяйте вашему ребенку встречаться с онлайн-знакомыми без вашего разрешения или в отсутствии взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу;
- Интересуйтесь тем, куда и с кем ходит ваш ребенок.

Объясните ребенку основные правила поведения в Сети:

- Нельзя делиться с виртуальными знакомыми персональной информацией, а встречаться с ними в реальной жизни следует только под наблюдением родителей.
- Если интернет-общение становится негативным – такое общение следует прервать и не возобновлять.

Как избежать кибербуллинга

Кибербуллинг – преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Предупреждение кибербуллинга:

- Объясните детям, что при общении в Интернете, они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов – читать грубости так же неприятно, как и слышать;
- Научите детей правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором и тем более пытаться ответить ему тем же. Возможно, стоит вообще покинуть данный ресурс и удалить оттуда свою личную информацию, если не получается решить проблему мирным путем;
- Если ребенок стал жертвой буллинга, помогите ему найти выход из ситуации – практически на всех форумах и сайтах есть возможность заблокировать обидчика, написать жалобу модератору или администрации сайта, потребовать удаление странички;
- Объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз;
- Старайтесь следить за тем, что ваш ребенок делает в Интернете, а также следите за его настроением после пользования Сетью.

Как защититься от кибербуллинга:

- Не провоцировать. Общаться в Интернете следует этично и корректно. Если кто-то начинает оскорблять ребенка в Интернете – необходимо порекомендовать уйти с такого ресурса и поискать более удобную площадку.

- Если по электронной почте или другим э-каналам кто-то направляет ребенку угрозы и оскорбления – лучше всего сменить электронные контакты (завести новый email, Skype, ICQ, новый номер мобильного телефона).
- Если кто-то выложил в Интернете сцену киберунижения ребенка, необходимо сообщить об этом администрации ресурса. Можно также обратиться на горячую линию. Даже при самых доверительных отношениях в семье родители иногда не могут вовремя заметить грозящую ребенку опасность и тем более не всегда знают, как ее предотвратить.

Вот на что следует обращать внимание родителям, чтобы вовремя заметить, что ребенок стал жертвой кибербуллинга:

- Беспокойное поведение. Даже самый замкнутый школьник будет переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и нежелание идти в школу – самые явные признаки того, что ребенок подвергается агрессии.
- Неприязнь к Интернету. Если ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В очень редких случаях детям действительно надоедает проводить время в Сети. Однако в большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире.
- Нервозность при получении новых сообщений. Негативная реакция ребенка на звук письма на электронную почту должна насторожить родителя. Если ребенок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.
- Как научить ребенка быть осторожным в Сети и не стать жертвой интернет-мошенников

Кибермошенничество – один из видов киберпреступления, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и другое)

Предупреждение кибермошенничества:

- Проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете;
- Установите на свои компьютеры антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных системах, наиболее частым из которых является кража конфиденциальных данных;
- Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности и, если ваш ребенок уже совершает онлайн-покупки самостоятельно, объясните ему простые правила безопасности:
- Ознакомьтесь с отзывами покупателей
- Проверьте реквизиты и название юридического лица – владельца магазина
- Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис WhoIs)
- Поинтересуйтесь, выдает ли магазин кассовый чек
- Сравните цены в разных интернет-магазинах.
- Позвоните в справочную магазина
- Обратите внимание на правила интернет-магазина
- Выясните, сколько точно вам придется заплатить
- Объясните ребенку, что нельзя отправлять слишком много информации о себе при совершении интернет-покупок: данные счетов, пароли, домашние адреса и номера телефонов. Помните, что никогда администратор или модератор сайта не потребует полные данные вашего счета, пароли и пин-коды. Если кто-то запрашивает подобные данные, будьте бдительны – скорее всего, это мошенники.

Как распознать интернет- и игровую зависимость

Сегодня в России все более актуальны проблемы так называемой «интернет-зависимости» (синонимы: интернет-аддикция, виртуальная аддикция) и зависимости от компьютерных игр («геймерство»). Первыми с ними столкнулись врачи-психотерапевты, а также компании, использующие в своей деятельности Интернет и несущие убытки, в случае если у сотрудников появляется патологическое влечение к пребыванию онлайн.

Как выявить признаки интернет-зависимости у ребенка:

- Оцените, сколько времени ребенок проводит в Сети, не пренебрегает ли он из-за работы за компьютером своими домашними обязанностями, выполнением уроков, сном, полноценным питанием, прогулками.
- Поговорите с ребенком о том, чем он занимается в Интернете. Социальные сети создают иллюзию полной занятости – чем больше ребенок общается, тем больше у него друзей, тем больший объем информации ему нужно охватить – ответить на все сообщения, проследить за всеми событиями, показать себя. Выясните, поддерживается ли интерес вашего ребенка реальными увлечениями, или же он просто старается ничего не пропустить и следит за обновлениями ради самого процесса. Постарайтесь узнать, насколько важно для ребенка общение в Сети и не заменяет ли оно реальное общение с друзьями.
- Понаблюдайте за сменой настроения и поведением вашего ребенка после выхода из Интернета. Возможно проявление таких психических симптомов как подавленность, раздражительность, беспокойство, нежелание общаться. Из числа физических симптомов можно выделить головные боли, боли в спине, расстройства сна, снижение физической активности, потеря аппетита и другие.

Если вы обнаружили возможные симптомы интернет-зависимости у своего ребенка, необходимо придерживаться следующего алгоритма действий:

- Постарайтесь наладить контакт с ребенком. Узнайте, что ему интересно, что его беспокоит и так далее.
- Не запрещайте ребенку пользоваться Интернетом, но постарайтесь установить регламент пользования (количество времени, которые ребенок может проводить онлайн, запрет на сеть до выполнения домашних уроков и прочее). Для этого можно использовать специальные программы родительского контроля, ограничивающие время в Сети.
- Ограничьте возможность доступа к Интернету только своим компьютером или компьютером, находящимся в общей комнате, – это позволит легче контролировать деятельность ребенка в сети. Следите за тем, какие сайты посещает ребенок.
- Попросите ребенка в течение недели подробно записывать, на что тратится время, проводимое в Интернете. Это поможет наглядно увидеть и осознать проблему, а также избавиться от некоторых навязчивых действий, например от бездумного обновления странички в ожидании новых сообщений.
- Предложите своему ребенку заняться чем-то вместе, постарайтесь его чем-то увлечь. Попробуйте перенести кибердеятельность в реальную жизнь. Например, для многих компьютерных игр существуют аналогичные настольные игры, в которые можно играть всей семьей или с друзьями, при этом общаясь друг с другом вживую. Важно, чтобы у ребенка были не связанные с Интернетом увлечения, которым он мог бы посвящать свое свободное время.
- Дети с интернет-зависимостью субъективно ощущают невозможность обходиться без Сети. Постарайтесь тактично поговорить об этом с ребенком. При случае обсудите с ним ситуацию, когда в силу каких-то причин он был вынужден обходиться без Интернета. Важно, чтобы ребенок понял – ничего не произойдет, если он на некоторое время выпадет из жизни интернет-сообщества.
- В случае серьезных проблем обратитесь за помощью к специалисту.

Как научить ребенка не загружать на компьютер вредоносные программы

Вредоносные программы (вирусы, черви, «троянские кони», шпионские программы, боты и др.) могут нанести вред компьютеру и хранящимся на нем данным. Они также могут снижать скорость

обмена данными и даже использовать ваш компьютер для распространения вируса, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Предупреждение столкновения с вредоносными программами:

- Установите на все домашние компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери данных. Такие приложения наблюдают за трафиком и могут предотвратить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.
- Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр.
- Объясните ребенку, как важно использовать только проверенные информационные ресурсы и не скачивать нелицензионный контент.
- Периодически старайтесь полностью проверять свои домашние компьютеры.
- Делайте резервную копию важных данных.
- Старайтесь периодически менять пароли (например, от электронной почты) и не используйте слишком простые пароли.

Что делать, если ребенок все же столкнулся с какими-либо рисками

- Установите положительный эмоциональный контакт с ребенком, расположите его к разговору о том, что случилось. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен вам доверять и знать, что вы хотите разобраться в ситуации и помочь ему, а не наказать;
- Постарайтесь внимательно выслушать рассказ о том, что произошло, понять, насколько серьезно произошедшее и насколько серьезно это могло повлиять на ребенка;
- Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети) или попал в неприятную ситуацию (потратил ваши или свои деньги в результате интернет-мошенничества и прочее) – постарайтесь его успокоить и вместе с ним разберитесь в ситуации: что привело к данному результату, какие неверные действия совершил сам ребенок, а где вы не рассказали ему о правилах безопасности в Интернете;
- Если ситуация связана с насилием в Интернете по отношению к ребенку, то необходимо выяснить информацию об агрессоре, выяснить историю взаимоотношений ребенка и агрессора, выяснить существует ли договоренность о встрече в реальной жизни; узнать были ли такие встречи и что известно агрессору о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и тому подобное), жестко настаивайте на избегании встреч с незнакомцами, особенно без свидетелей, проверьте все новые контакты ребенка за последнее время;
- Соберите наиболее полную информацию о происшествии, как со слов ребенка, так и с помощью технических средств: зайдите на страницы сайта, где был ваш ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию – в дальнейшем это может вам пригодиться (например, для обращения в правоохранительные органы);
- Если вы не уверены в оценке серьезности произошедшего с вашим ребенком, или ребенок недостаточно откровенен с вами или вообще не готов идти на контакт, или вы не знаете как поступить в той или иной ситуации – обратитесь к специалисту (телефон доверия, горячая линия и другое), где вам дадут рекомендации о том, куда и в какой форме обратиться, если требуется вмешательство других служб и организаций (МВД, МЧС, Сестры и другие)

Линия помощи “Дети Онлайн”

Если вы нуждаетесь в консультации специалиста по вопросам безопасного использования Интернета или если ваш ребенок уже столкнулся с рисками в Сети, обратитесь на линию помощи “Дети Онлайн” по телефону: 8 800 25 000 15 (звонок по России бесплатный). На линии помощи профессиональную психологическую и информационную поддержку оказывают психологи факультета психологии МГУ имени М.В.Ломоносова и Фонда Развития Интернет. Источник: http://www.google.ru/goodtoknow/familysafety/advice/

Как родителям защитить детей от опасностей интернета?

Современные дети с малых лет знакомы с Интернетом. Многие родители знают, что в сети ребят подстерегают различные опасности. В статье мы собрали материал о том, какие существуют угрозы в интернете и как родители могут защитить своих детей от этих опасностей путем установления правил, бесед и при помощи специальных программ.

Чем опасен Интернет для детей и подростков: виды угроз

Основные виды угроз в интернете для детей:

- **Сайты, связанные с сексом.** В интернете полно сервисов, где пропагандируют нездоровые сексуальные отношения: секс за деньги, разные развращения, гомосексуализм. От этого нужно оградить своих детей, особенно, если они еще маленькие и многого не понимают.
- **Сайты, распространяющие информацию о запрещенных вещах и понятиях.** К таким относятся терроризм, сектантство, фашизм и т. д. Такой контент может сильно навредить слабой психики ребенка.
- **Игры.** Во-первых, во многих играх присутствуют насилие, убийства. Во-вторых, игры начинают заменять реальный мир, ребенку все тяжелее выходить из игры, особенно, если он чувствовал себя настоящим героем в игре и у него там куча друзей.
- **Азартные игры**. Они обещают большие деньги за короткий срок. А ведь ребенку гораздо сложнее устоять перед таким соблазном, чем взрослым. Под влиянием жажды выигрыша ребенок может начать спускать родительские деньги.
- **Форумы, социальные сети, сайты знакомств** затягивают ребенка в виртуальный мир. У него в сети возникает дружба с кучей людей, он там отлично общается. А в реальности у ребенка могут проблемы с общением со сверстниками.
- **В сети много мошенников** и им легче подобраться к нам и нашим детям. Есть много способов обмануть человека. Рассмотрим один из популярных способов обмана в сети. На сайте просят ввести номер сотового, потом приходит смс-ка о выигрыше крупной суммы денег. Чтобы их получить, мошенники просят отправить смс со своего телефона на другой номер. В итоге с вашего мобильного счета списывается приличная сумма.
- **Обман в реальном мире**. Через интернет любой человек может познакомиться с вашим ребенком, например, под видом симпатичной девушки и назначить ему свидание. Ваш ребенок приходит на место встречи, а к нему подходит неизвестный мужчина, представляется отцом девушки и уговаривает отвезти его к ней, так как она заболела. В этом случае с ним может произойти всякое. Поэтому, учите своего ребенка не доверять незнакомцам.

Как обеспечить безопасность детей в интернете – советы для родителей

Таблица. Как защитить детей от опасностей интернета?

Виды опасностей в интернете	Как родителям предупредить столкновение ребенка с опасностями в интернете?	Как действовать родителям при столкновении ребенка с определенной опасной ситуацией в сети?
Нежелательный контент	Расскажите своим детям, что в интернете много неправдоподобной информации. Научите их интересоваться у вас, если они что-то не так поняли. Обязательно спрашивайте, что ребенок видел в Интернете. Часто проис-	В семье должны быть правила по пользованию интернетом. Благодаря этому ребенок четко будет знать, что делать, если он столкнулся с нежелательным контентом.

	ходит так, что ему становится интересен один сайт, он начинает открывать другие подобные сайты. Стоит включить программу родительского контроля и безопасного поиска. Они помогут в борьбе с нежелательным контентом.	Интересуйтесь у ребенка, что он ищет в интернете.
Интернет— знакомства	Вы должны знать, с кем ребенок общается в интернете, проверяйте его контакты, чтобы знать с кем он общается. Если вы заметили, что ребенок часто общается с людьми старше своего возраста, то следует с ним об этом поговорить. Не стоит позволять ребенку встречаться со знакомым из интернета без вашего разрешения. Если он горит желанием встретиться с кем-то из виртуальных знакомых, то вам стоит обязательно сопроводить своего ребенка. Вы должны знать где бывает ваш ребенок, с кем он туда ходит.	Объясните ребенку следующие правила: 1)Не стоит давать знакомому личную информацию о себе. А знакомство с виртуальным знакомым должно проходить под присмотром родителей. 2) Если становится не по себе при общении со знакомым в интернете, убедите его порвать такое общение.
Кибербуллинг	Поговорите с ребенком и убедите его общаться в интернете вежливо и без грубостей. Учите его адекватно реагировать на сообщения от других людей. Объясните ему, что не стоит продолжать общение с человеком, который проявляет агрессию. Если ребенка обидели, то помогите ему выйти из этой ситуации. На любом форуме или сайте можно заблокировать этого человека либо написать на него жалобу модератору. Объясните ему, что в интернете нельзя угрожать либо распространять сплетни. Следите, чем занимается ребенок в сети. Наблюдайте за его настроением после использования интернета.	Если ребенок получает на электронную почту или другие сервисы оскорбления, стоит поменять контакты в интернете. Если вы обнаружили в сети картину киберунижения вашего ребенка, обязательно обратитесь в администрацию сервиса либо позвоните на горячую линию.
Кибермошенничество	Расскажите ребенку о видах мошенничества и убедите его обращаться к взрослым за советом, если он желает воспользоваться какой-то услугой в сети. Стоит установить на свой компьютер антивирус либо персональный брандмауэр.	Если ваш ребенок хочет сделать покупку в интернет-магазине, то расскажите ему о правилах безопасности. Стоит проверить все данные о магазине (реквизиты, название юридического лица). Узнайте, доставляет ли интернет-магазин кассовый чек. Внимательно ознакомьтесь с правилами магазина. Уточните, сколько точно надо будет

		заплатить за товар. Расскажите ребенку, что не стоит давать всю информацию о себе, когда покупаешь вещь в интернет-магазине.
Игровая и интернет-зависимость	Понаблюдайте за ребенком и проанализируйте, сколько времени он находится в интернете ежедневно. Пообщайтесь с ребенком, поинтересуйтесь чем он занят в сети. Не пренебрегает ли он своими реальными увлечениями в жизни: занимается ли любимым спортом, читает ли книги и др. Посмотрите на его настроение после каждого выхода из интернета. Если он в плохом настроении, агрессивен, раздражителен и не хочет ни с кем разговаривать — это говорит об интернет — зависимости.	Почаще общайтесь с ребенком, проявляйте интерес к его личной жизни, играйте с ним. Нельзя запрещать ему использовать интернет, но стоит ограничить его пребывание в нем. Разрешайте ему пользоваться только своим компьютером или компьютером, который находится в общей комнате для лучшего контроля пребывания ребенка в интернете. Если вы видите, что ребенок привязался к интернету и практически не может без него. Убедите его в том, что ничего такого не будет, если он несколько часов отдохнет от интернета.
Вредоносные программы	Надо установить на все компьютеры специализированные почтовые фильтры и антивирусные программы. Стоит использовать лицензионные программы и данные только из проверенных мест. Поясните ребенку, что не стоит скачивать все подряд, а только проверенную информацию. Каждую неделю проверяйте компьютеры на наличие вирусов. Обязательно копируйте важные документы на флешку или диск. Раз в три месяца меняйте пароли в своих аккаунтах и не пользуйтесь излишне простыми паролями.	Общайтесь с ребенком благожелательно. Расположите его к себе, он должен вам доверять. Внимательно слушайте ребенка, если что-то произошло. Попытайтесь понять насколько сильно это повлияло на него. Если же ребенок совершил ошибку и его взломали в социальной сети или он решил что-то купить в интернете и наткнулся на обман, то не стоит его сильно ругать. Надо просто вместе разобраться и спокойно объяснить ему правила действий в интернете. Если ребенку угрожают в интернете, то надо узнать всю информацию об этом человеке. Спросить у ребенка, встречался ли он с ним. Обязательно стоит настаивать на том, что с незнакомыми людьми встречаться нельзя. Можно попробовать собрать побольше информации об этом человеке, скопировать сообщения, которые он присылал и обратиться в полицию. Если вы заметили, что ребенок чего-то не говорит или вы не можете понять, что произошло, обратитесь к специалистам, где вам подскажут, какие действия предпринять в этой ситуации.

Программа «Родительский контроль» — помощь в обеспечении безопасности ребенка в интернете

Программ для родительского контроля детей в интернете достаточно много. Рассмотрим некоторые из них.

- **Платная программа KinderGate Родительский контроль** блокирует сайты для взрослых, есть настройки для ограничения доступа к игровым сайтам, сайтам с насилием или наркотиками и т. п. Можно установить расписание, когда ребенок сможет сидеть в интернете. Можно увидеть на какие сайты он заходит.
- **Бесплатный браузер детский интернет фильтр КиберПапа.** Тут включается фильтр и ребенок заходит только на детские сайты, которые тщательно проверены. Выключить его смогут только родители, зная пароль.
- **Платная программа КиберМама.** Можно создать время, когда ребенок может находиться в сети. Все это контролируется. Также можно заблокировать доступ в интернете.
- **Бесплатный детский браузер Гогуль.** В этом браузере есть свои детские сайты. Здесь составляется время, когда ребенок может посидеть в интернете. Можно ограничить посещение интернета. Родители получают полный отчет, на каких сайтах были их дети.
- **NetKids.** Родители просматривают все сайты, которые посещает их ребенок. Также они могут блокировать опасные сайты.
- **Платная программа KidsControl.** Тут можно вручную ограничить доступ к сомнительным ресурсам, контролировать время нахождения ребенка в интернете.

Советы специалистов по безопасности детей в интернете

Первое, что необходимо сделать родителям, научить ребенка никому не сообщать пароли. Скажите ребенку: «Никогда не сообщай свои пароли другим, даже друзьям. Храни записанные пароли в недоступном месте. Никогда не сообщай свой пароль по электронной почте.» (**А.Левченко**, помощник Уполномоченного по правам ребенка при Президенте РФ, директор НП Мониторинговый центр по выявлению опасного и запрещенного законодательством контент)

Немаловажно научить ребенка не делиться информацией личного характера в сети, не публиковать конфиденциальные данные. Излишняя откровенность в Интернете чревата. При этом важно помнить, что персональные сведения могут стать доступными ненамеренно: используя функции автозаполнения, разрешая приложениям отслеживать местоположение, заполняя графы с указанием адреса и телефона, ребенок подвергает себя дополнительной опасности. Контакт родителей с детьми — ключевой фактор, от которого зависит поведение подростка в виртуальной жизни. Родители должны ориентироваться в социальных сетях, знать, на каких сайтах и как проводят время их дети, а, кроме того, совершенствовать собственный уровень технической осведомленности.(**Р. Вераксич,** эксперт в области безопасности McAfee, подразделения Intel Security)

Побольше общайтесь со своими детьми, завоевывайте их доверие, интересуйтесь их делами, вовлекайте их в семейные игры, ходите с ними на погулки на свежем воздухе. Тогда ваш ребенок не захочет подолгу сидеть в интернете, потому что реальная жизнь для него будет интереснее виртуальной.