Дети в Интернете: правила безопасности

круглосуточная телефонная линия «ребенок в опасности»

8-8152-**42-01-32;**

телефон доверия **8-921-040-07-04**

Зачастую дети и подростки в полной мере не осознают все возможные проблемы, с которыми они могут столкнуться в сети. Сделать их пребывание в интернете более безопасным, научить их ориентироваться в киберпространстве — важная задача для их родителей.

Чтобы обезопасить юного пользователя, родителям нужно обозначить границы дозволенного и возможные опасности.

Основные правила безопасности для родителей:

- Прежде, чем позволить ребенку пользоваться Интернетом, расскажите ему о возможных опасностях Сети (вредоносные программы, небезопасные сайты, интернет-мошенники и др.) и их последствиях.
- Четко определите время, которое Ваш ребенок может проводить в Интернете, и сайты, которые он может посещать.
- Убедитесь, что на компьютерах установлены и правильно настроены антивирусные программы, средства фильтрации контента и нежелательных сообщений.

- Контролируйте деятельность ребенка в Интернете с помощью специального программного обеспечения.
- Спрашивайте ребенка о том, что он видел и делал в Интернтете.
- Объясните ребенку, что при общении в Интернете (чаты, форумы, сервисы мгновенного обмена сообщениями, онлайн-игры) и других ситуациях, требующих регистрации, нельзя использовать реальное имя. Помогите ему выбрать регистрационное имя, не содержащее никакой личной информации.
- Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также "показывать" свои фотографии.
- Помогите ребенку понять, что далеко не все, что он может прочесть или увидеть в Интернете — правда. Приучите его спрашивать то, в чем он не уверен.
- Объясните ребенку, что нельзя открывать файлы, полученные от неизвестных пользователей, так как они могут содержать вирусы или фото/видео с негативным содержанием.
- Приучите ребенка советоваться со взрослыми и немедленно сообщать о появлении нежелательной информации.
- Не позволяйте Вашему ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствии взрослого человека.
- Постарайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они знают всех, с кем они общаются;
- Объясните детям, что при общении в Интернете, они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов — читать грубости также неприятно, как и слышать;
- Проверяйте актуальность уже установленных правил. Следите за тем, чтобы Ваши правила соответствовали возрасту и развитию Вашего ребенка.

Виды интернет-угроз

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов. Английское слово буллинг (bullying, от bully — драчун, задира, грубиян, насильник) обозначает запугивание, унижение, травлю, физический или психологический террор, направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе.

В современном информационном обществе для буллинга все чаще используются инфокоммуникационные технологии. Буллинг, осуществляемый в виртуальной среде с помощью интернета и мобильного телефона, называют кибербуллингом. Основной площадкой для кибербуллинга в последнее время являются социальные сети. В них можно оскорблять человека не только с помощью сообщений – нередки случаи, когда страницу жертвы взламывают (или создают поддельную на ее имя), где размещают лживый и унизительный контент.

Как справляться с кибербуллингом:

- Проговорите с ребенком ситуацию и внимательно его выслушайте. Выясните у ребенка всю возможную информацию.
- Сохраните все возможные свидетельства происходящего (скриншоты экрана, электронные письма, фотографии и т.п.).
- Сохраняйте спокойствие — вы можете еще больше напугать ребенка своей бурной реакцией на то, что он вам рассказал и показал. Главной задачей является эмоциональная поддержка ребенка. Нужно дать ему уверенность в том, что проблему можно преодолеть. Никогда не наказывайте и не ограничивайте действия ребенка в ответ на его признание.
- Повторите ребенку простейшие правила безопасности при пользовании интернетом, дайте советы по дальнейшему предотвращению кибер-буллинга.

Встречи с незнакомцами и груминг

Общаясь в сети, дети могут знакомиться, общаться и добавлять в «друзья» совершенно неизвестных им в реальной жизни людей. В таких ситуациях есть опасность разглашения ребенком личной информации о себе и своей семье. Также юный пользователь рискует подвергнуться оскорблениям, запугиванию и домогательствам. Особенно опасным может стать груминг – установление дружеских отношений с ребенком с целью личной встречи, вступления с ним в сексуальные отношения, шантажа и эксплуатации. Такие знакомства чаще всего происходят в

чате, на форуме или в социальной сети. Общаясь лично («в привате»), злоумышленник, чаще всего представляясь сверстником, входит в доверие к ребенку, а затем пытается узнать личную информацию (адрес, телефон и др.) и договориться о встрече. Иногда такие люди выманивают у детей информацию, которой потом могут шантажировать ребенка, например, просят прислать личные фотографии или провоцируют на непристойные действия перед веб-камерой.

Как противостоять грумингу:

- Если ребенок желает познакомиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу
- Проговорите с ребенком ситуацию и внимательно его выслушайте. Выясните у ребенка всю возможную информацию
- Сохраняйте спокойствие — вы можете еще больше напугать ребенка своей бурной реакцией на то, что он рассказал или показал. Главной задачей является эмоциональная поддержка ребенка. Нужно дать ребенку уверенность в том, что проблему можно преодолеть. Никогда не наказывайте и не ограничивайте действия ребенка в ответ на его признание.
- Сохраните все свидетельства переписки и контактов незнакомца с ребенком (скриншоты экрана, электронные письма, фотографии и т.п.).
- При обнаружении признаков совращения следует немеделенно сообщить об этом в правоохранительные органы
- Повторите ребенку простейшие правила безопасности при пользовании интернетом, дайте советы по дальнейшему предотвращению груминга.

Контентные риски

К контентным рискам относятся материалы (тексты, картинки,аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию. В первую очередь, с таким контентом можно столкнуться на сайтах социальных сетей, в блогах, на торрентах. Но сегодня практически весь интернет - это виртуальное пространство риска.

Противозаконный контент - распространение наркотических веществ через интернет, порнографические материалы с участием несовершеннолетних, призывы к разжиганию национальной розни и экстремистским действиям.

Вредоносный (опасный) контент - контент, способный нанести прямой вред психическому и физическому здоровью детей и подростков.

Неэтичный контент - контент, который не запрещен к распространению, но может содержать информацию,способную оскорбить пользователей. Подобное содержимое может распространяться ограниченно (например, "только для взрослых").

Особо опасны сайты, на которых обсуждаются способы причинения боли и вреда, способы чрезмерного похудения, способы самоубийства, сайты, посвященные наркотикам, сайты, на которых размещены полные ненависти сообщения, направленные против отдельных групп или лиц. Столкновения с контентными рисками могут иметь негативные последствия для эмоциональной сферы, психологического развития, социализации, а также физического здоровья детей и подростков.

Рекомендации по предупреждению контентных рисков:

- Используйте специальные технические средства, чтобы ограничивать доступ ребенка к негативной информации – программы родительского контроля и контентной фильтрации, настройки безопасного поиска. Часто пакет функций родительского контроля уже есть в вашей антивирусной программе. Программы родительского контроля позволяют: установить запрет на посещения сайтов различного негативного содержания, сайтов онлайн-знакомств, сайтов с вредоносным содержимым; ограничить время доступа ребенка к интернету; производить мониторинг переписки в социальных сетях и онлайн мессенджерах (чатах); блокировать сомнительные поисковые запросы в поисковых системах; блокировать баннеры; а также отслеживать все действия ребенка в сети.
- Если ребенок пользуется общим компьютером, для каждого члена семьи создайте свою учетную запись на компьютере. Ваша учетная запись должна иметь надежный пароль и обладать правами администратора, чтобы ребенок не мог менять установленные вами настройки и программы.
- Регулярно следите за активностью вашего ребенка в сети. Просматривайте историю посещений сайтов, чтобы быть уверенным, что среди них нет опасных. При необходимости обновляйте настройки технических средств безопасности.
- Объясните детям, что далеко не все, что они могут прочесть или увидеть в интернете – правда. Необходимо проверять информацию,

увиденную в интернете. Для этого существуют определенные правила проверки достоверности информации. Признаки надежного сайта, информации которого можно доверять, включают: авторство сайта, контактные данные авторов, источники информации, аккуратность представления информации, цель создания сайта, актуальность данных. Расскажите об этих правилах вашим детям.

- Поддерживайте доверительные отношения с вашим ребенком, чтобы всегда быть в курсе с какой информацией он сталкивается в сети. Попав случайно на какой-либо опасный, но интересный сайт, ребенок может продолжить поиск подобных ресурсов. Важно заметить это как можно раньше и объяснить, ребенку, чем именно ему грозит просмотр подобных сайтов.
- Важно помнить, что невозможно всегда находиться рядом с детьми и постоянно их контролировать. Доверительные отношения с детьми, открытый и доброжелательный диалог зачастую могут выступать более эффективными средствами для обеспечения безопасности вашего ребенка, чем постоянное отслеживание посещаемых сайтов и блокировка всевозможного контента.

Помните, что главным в предупреждении опасности ребенка остается одно – это доверительное отношение ребенка к родителям. Важно почувствовать грань между внимательным отношением и агрессивным вмешательством в жизнь подростка. Ведь эта крайность может привести к не менее печальным последствиям.

Среди детей популярна новомодная игра: "Беги или умри!". Суть этой игры: перебежать дорогу как можно ближе перед движущимся транспортом. Эта игра популярна по всей России. Поэтому и водителям нужно быть предельно внимательными, когда видите детей у дороги и учитывать тот факт, что они могут броситься бежать прямо под колёса. Также появились группы в социальных сетях, в которых дети "покупают" свою смерть! Приобретая приложение, за ними закрепляется человек, следящий за выполнением заданий, последним этапом игры - является суицид.

На что следует обратить внимание:

1. Подросток не высыпается, даже если рано ложится спать - проследите, спит ли он в ранние утренние часы.

2. Рисует китов, бабочек, единорогов.

3. Состоит в группах, содержащих в названии следующее: "Киты плывут вверх", "Разбуди меня в 4.20", f57, f58, "Тихийдом", "Рина ", "Няпока", "Море китов", "50 дней до моего..."

хэштеги: домкитов, млечныйпуть, 150звёзд, ff33, d28, хочувигру.

4. Закрыл в Контакте доступ к подробной информации, в переписке с друзьями (на личной стене) есть фразы "разбуди меня в 4.20", "я в игре". И совсем уж страшно, если на стене появляются цифры, начиная от 50 и меньше.

5. Переписывается в вайбере (и др. мессенджерах) с незнакомыми людьми, которые дают странные распоряжения.

7 советов по компьютерной безопасности для учащихся:

Обычно подготовка к школе заключалась в укладывании в портфель карандашей, тетрадей и учебников. Сегодня в начале этого списка нередко находится компьютер. Ознакомьтесь с этими советами, чтобы защитить компьютеры, которыми вы пользуетесь в школе, от вирусов, хакеров, программ-шпионов и других возможных атак.

1. Соблюдайте основные меры компьютерной безопасности!

Перед тем, как отправиться в путешествие по интернету, необходимо выполнить три важных действия для усиления компьютерной защиты.

1. Активизации брандмауэра
2. Обновления антивирусных программ
3. Обновления программного обеспечения

2. Не открывайте файлы, полученные от неизвестных корреспондентов!

Электронная почта и мгновенные сообщения позволяют быстро обменяться информацией с друзьями, родственниками и одноклассниками. Но если не проявить необходимой осторожности, электронная почта и мгновенные сообщения могут распространить вирусы и черви. Основная масса вредоносных программ попадает в компьютер через электронную почту теми, кто нечаянно попытался открыть зараженный файл. Не дайте себя одурачить! Ни в коем случае нельзя открывать файл, вложенный в письмо электронной почты или мгновенное сообщение, если его отправитель неизвестен и вы не ожидаете получения файла.

3. Как бороться со спамом и сетевыми мошенниками!

Нужно также освоить способы борьбы со спамом и сетевым мошенничеством. Мошенничество phishing представляет собой еще одну угрозу конфиденциальности ваших данных. У вас могут украсть номер кредитной карты, пароли, учетную информацию или другие личные данные.

4. Как защититься от программ-шпионов!

Ваш браузер погряз во всплывающих окнах? На экране компьютера появились панели, которые вы не загружали? Возможно, вы стали жертвой программы-шпиона. Она занимается сбором вашей личной информации, не предупреждая об этом и не спрашивая на то разрешения. Получить эту вредоносную программу можно при скачивании музыки или программ обмена файлами; загрузки бесплатных игр с подозрительных сайтов или других программ.

5. Принимайте необходимые меры предосторожности, пользуясь беспроводной связью!

В настоящее время многие учебные заведения оснащены беспроводными сетями. Это дает возможность путешествовать по интернету, находясь в библиотеке, кафе или учебной аудитории. Возможно, вы уже пользовались беспроводными сетями дома, в аэропорту, кафетериях или даже общественных парках. Такие сети очень удобны, но их использование сопряжено со снижением уровня безопасности.

6. Пароль защищает ваш компьютер и блокирует возможность его использования!

Пароли являются первой линией защиты от злоумышленников, шутников или беспечного соседа по комнате. Если вы не пользуетесь паролем для входа в компьютер, кто угодно может получить доступ. (Чтобы «запереть» компьютер с операционной системой Windows, удерживайте нажатыми клавиши «Windows + L». Когда понадобится возобновить работу, следуйте инструкциям на экране)

7. Делайте резервные копии результатов работы (а также игр и других развлекательных программ)!

Образ студента, оставшегося без своей курсовой работы из-за того, что он забыл сделать резервную копию, стал уже почти штампом. Тем не менее многие до сих пор не находят времени на копирование. Пользователи Windows XP, могут воспользоваться программой Архивация данных, которая выполнит за вас эту работу.