Рекомендации учителям и родителям о том, как обеспечить безопасность ребенка в Интернете

Компания Google представляет практические рекомендации о том, как помочь юным пользователям оставаться в безопасности в киберпространстве и избежать существующих рисков.

Как защитить ребенка от нежелательного контента в Интернете

Фонд Развития Интернет

Контентные риски – это материалы (тексты, картинки, аудио- и 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, является правдой. 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.

Центр безопасного Интернета в России

- 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

Фонд Развития Интернет

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

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 другое. В других случаях они могут оказаться преступниками в поисках жертвы. Специалисты используют 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.

По европейским данным, значимость проблемы «встречи с онлайн-незнакомцами» во многих странах Европы существенно снизилась. В России этот вопрос остается одним из самых важных среди коммуникационных интернет-рисков. Половина российских детей постоянно знакомится в Интернете с новыми людьми, а 22% детей признаются, что встречались с интернет-знакомыми в реальной жизни. В Европе знакомятся в Интернете 29% детей, но встречаются с онлайн-знакомыми в реальности меньше - около 10%.

Предупреждение груминга:

- Будьте в курсе того, 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 отсутствие 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.

Центр безопасного Интернета в России

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

Фонд Развития Интернет

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. Особенно остро переживают кибербуллинг дети 9-10 лет: 52% детей этого возраста, ставшие жертвой подобной ситуации, в первую очередь девочки, указали на то, что были этим сильно или очень сильно расстроены.

Кроме того, нередко и сами школьники выступают агрессорами. В России 25% детей признались, что за последний год обижали или оскорбляли других людей в реальной жизни или в Интернете. Обращает на себя внимание тот факт, что в России субъектов буллинга в два раза больше, чем в среднем по европейским странам. При этом и российские, и европейские школьники чаще сознаются, что проявляли агрессию лицом к лицу (16% в России и 10% в ЕС), но гораздо реже признаются, что вели себя агрессивно в Интернете (6% в России и 3% в ЕС).

Кибербуллинг – преследование при помощи сообщений, содержащих 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 и ни в коем случае не должны писать грубые слова – 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 страницы.

■ 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.

По данным, полученным в исследовании «Дети России онлайн», в среднем по России 23% детей, которые пользуются Интернетом, являются жертвой буллинга онлайн или офлайн. В Европе дети в среднем не намного реже, чем в России, признаются, что стали жертвой буллинга (19%). Пятая часть российских детей – жертв буллинга подвергается обидам и унижениям либо каждый день, либо 1-2 раза в неделю. Особенно актуальна эта проблема для детей 11-12 лет: почти треть детей – жертв буллинга этой возрастной группы подвергается оскорблениям чаще одного раза в неделю.

Новые инфокоммуникационные технологии предоставляют дополнительные возможности для буллинга, и российские дети этим пользуются. Если сравнить виртуальность и реальность, то российские дети подвергаются буллингу в Интернете так же часто, как и в реальной жизни. Оскорбления в чатах, на форумах, в блогах и в комментариях к ним, поддельные страницы или видеоролики с элементами насилия стали привычной частью Рунета – каждый десятый ребенок 9-16 лет становился жертвой кибербуллинга. В европейских странах дети подвергаются кибербуллингу в Интернете в два раза реже.

Центр безопасного Интернета в России

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 онлайн-каналам кто-то направляет ребенку угрозы и оскорбления, лучше всего сменить электронные контакты (завести новый email, Skype, ICQ, новый номер мобильного телефона).

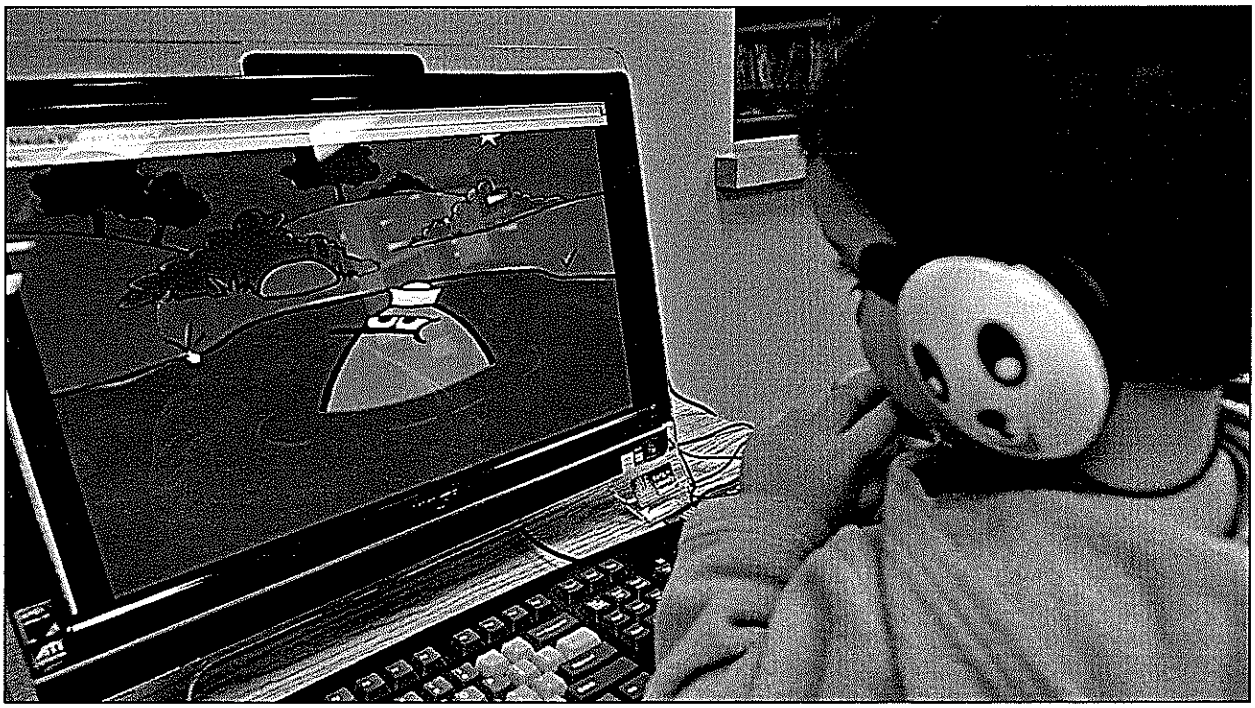
■ Если кто-то выложил в Интернете сцену киберунижения ребенка, необходимо сообщить об этом администрации ресурса. Можно также обратиться на горячую линию.

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 приходящего на электронную почту письма 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

Фонд Развития Интернет

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 Whols).

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 администратор или модератор сайта никогда 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

Фонд Развития Интернет

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, которое 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 вре-

мя, 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

Фонд Развития Интернет

Вредоносные программы (вирусы, черви, «троянские кони», шпионские программы, боты и другие) могут нанести вред компьютеру и хранящимся в 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

Фонд Развития Интернет

■ 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), твердо 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, и другие).