Актуальные рекомендации о безопасном интернете

1. 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.

2. 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.

3. 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.

4. 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:

1. Ознакомьтесь с отзывами покупателей
2. Проверьте реквизиты и название юридического лица – владельца магазина
3. Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис WhoIs)
4. Поинтересуйтесь, выдает ли магазин кассовый чек
5. Сравните цены в разных интернет-магазинах.
6. Позвоните в справочную магазина
7. Обратите внимание на правила интернет-магазина
8. 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.

5. Как распознать интернет- и игровую зависимость?

Сегодня в России все более актуальны проблемы так называемой «[интернет-зависимости](http://www.debotaniki.ru/2011/04/komputernaya-zavisimost-detey/)» (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:

1. Постарайтесь наладить контакт с ребенком. Узнайте, что ему интересно, что его беспокоит и так далее.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. В случае серьезных проблем обратитесь за помощью к специалисту.