Родителям: Безопасность школьников в интернете

Чтобы помочь своим детям, вы должны это знать:

1. Будьте в курсе того, чем занимаются ваши дети в интернете. Попросите их научить вас пользоваться различными приложениями, которыми вы не пользовались ранее.

2. Помогите своим детям понять, что они не должны предоставлять никому информацию о себе в интернете – номер мобильного телефона, домашний адрес, название/номер школы, а также показывать фотографии свои и семьи. Ведь любой человек в интернете может это увидеть.

3. Если ваш ребенок получает спам (нежелательную электронную почту), напомните ему, чтобы он не верил написанному в письмах и ни в коем случае не отвечал на них.

4. Объясните детям, что нельзя открывать файлы, присланные от неизвестных вам людей. Эти файлы могут содержать вирусы или фото/видео с «агрессивным» содержанием.

5. Помогите ребенку понять, что некоторые люди в интернете могут говорить неправду и быть не теми, за кого себя выдают. Дети никогда не должны встречаться с сетевыми друзьями в реальной жизни самостоятельно без взрослых.

6. Постоянно общайтесь со своими детьми. Никогда не поздно рассказать ребенку, как правильно поступать и реагировать на действия других людей в интернете.

7. Научите своих детей, как реагировать в случае, если их кто-то обидел или они получили/натолкнулись на агрессивный контент в интернете, так же расскажите, куда в подобном случае они могут обратиться.

8. Убедитесь, что на компьютерах установлены и правильно настроены средства фильтрации.

Возможные опасности, с которыми сопряжен доступ детей к интернету

1. *Неприемлемые материалы*. В интернете ребенок может столкнуться с материалами, связанными с сексом, провоцирующими возникновение ненависти к кому-либо или побуждающими к совершению опасных либо незаконных действий.

2. *Неприятности, связанные с нарушением законов или финансовыми потерями*. У ребенка могут обманным путем узнать номер вашей кредитной карточки, и это вызовет финансовые потери. Ребенка также могут склонить к совершению поступков, нарушающих права других людей, что в конечном счете приведет к возникновению у вашей семьи проблем, связанных с нарушением законов.

3. *Разглашение конфиденциальной информации*. Детей и даже подростков могут уговорить сообщить конфиденциальную информацию. Сведения личного характера, такие как имя и фамилия ребенка, его адрес, возраст, пол и информация о семье, могут легко стать известными злоумышленнику. Даже если сведения о вашем ребенке запрашивает заслуживающая доверия организация, вы все равно должны заботиться об обеспечении конфиденциальности этой информации.

4. *Проблемы технологического характера*. По недосмотру ребенка, открывшего непонятное вложение электронной почты или загрузившего с веб-узла

небезопасный код, в компьютер может попасть вирус, «червь», «троян», «зомби» или другой код, разработанный со злым умыслом.

Меры предосторожности:

1. *Побеседуйте с детьми*. Первое, что необходимо сделать, – это объяснить им, что нахождение в интернете во многом напоминает пребывание в общественном месте. Многие опасности, подстерегающие пользователя интернета, очень схожи с риском, возникающим при общении с чужими людьми, и дети должны понимать, что, если они не знают человека, с которым вступили в контакт лично, это означает, что они общаются с незнакомцем, что запрещено и в реальной, а не только в виртуальной действительности.

2. *Разработайте правила пользования интернетом*:

1) четко объясните детям, посещение каких веб-узлов является приемлемым и какими правилами нужно руководствоваться при пользовании интернетом. Приведите ясные и наглядные примеры того, что следует искать, и убедитесь в том, что дети обратятся к вам, если столкнутся с не внушающими доверия или смущающими их материалами;

2) пароли. Предупредите детей о том, что они не должны никому сообщать свои пароли, даже если человек утверждает, что является сотрудником вашего поставщика интернет-услуг (например, представляется вашим провайдером). Поставщик услуг интернета никогда не будет спрашивать, какой у вас пароль;

3) разработайте «домашнюю» политику. Составьте список того, что можно и чего нельзя делать любому члену вашей семьи при использовании интернета. Например: нельзя разглашать информацию личного характера. Объясните детям, что они не должны сообщать свою фамилию, адрес, номер телефона или давать свою фотографию. Ребенок ни в коем случае не должен соглашаться на личную встречу с виртуальным другом без разрешения и присутствия родителей. Нельзя ничего покупать через веб-узел, деятельность которого осуществляется через небезопасный сервер. Перед тем как совершить покупку, необходимо всегда спрашивать разрешения взрослых;

4) следует либо не допускать использования ребенком чата, либо контролировать это занятие. Кроме того, нужно убедиться в том, что выбранный им чат является управляемым и поддерживается заслуживающей доверия компанией или организацией;

5) установите компьютер в помещении, используемом всеми членами семьи, а не в комнате ребенка. Это упростит контроль за пребыванием детей в интернете. Воспользуйтесь современными технологиями;

6) контролируйте входящие и исходящие сообщения электронной почты своего ребенка. Знакомьтесь с его виртуальными друзьями подобно тому, как вы знакомитесь с реальными;

7) регулярно просматривайте журнал веб-обозревателя. Из него вы узнаете, какие веб-узлы посещали ваши дети и как часто они это делали;

8) настройте веб-обозреватель в режиме обеспечения безопасности.

Помните!

Эти простые меры, а также доверительные беседы с детьми о том, каких правил им следует придерживаться при использовании интернета, позволят вам чувствовать себя спокойно, отпуская ребенка в познавательное и безопасное путешествие по Всемирной сети.

Рекомендации родителям, как сделать посещение интернета для детей полностью безопасным:

1. Поощряйте детей делиться с вами их опытом в интернете. Посещайте Сеть вместе с детьми.

2. Научите детей доверять интуиции. Если их в интернете что-либо беспокоит, им следует сообщить об этом вам.

3. Если дети общаются в чатах, используют программы мгновенного обмена сообщениями, играют или занимаются чем-то иным, требующим регистрационного имени, помогите ребенку его выбрать и убедитесь, что оно не содержит никакой личной информации.

4. Настаивайте на том, чтобы дети никогда не выдавали своего адреса, номера телефона или другой личной информации; например, места учебы или любимого места для прогулки.

5. Объясните детям, что разница между правильным и неправильным одинакова: как в интернете, так и в реальной жизни.

6. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.

7. Настаивайте, чтобы дети уважали собственность других в интернете. Объясните, что незаконное копирование чужой работы – музыки, компьютерных игр и других программ – является кражей.

8. Скажите детям, что им никогда не следует встречаться с друзьями из интернета. Объясните, что эти люди могут оказаться совсем не теми, за кого себя выдают.

9. Скажите детям, что не все, что они читают или видят в интернете, правда. Приучите их спрашивать вас, если они не уверены.

10. Контролируйте деятельность детей в интернете с помощью современных программ. Они помогут отфильтровать вредное содержимое, выяснить, какие сайты посещает ребенок и что он делает на них.

Советы по достижению равновесия между временем, проводимым в интернете и вне его:

1. *Следите за симптомами проявления интернет-зависимости*. Спросите себя: оказывает ли времяпрепровождение в Сети влияние на школьные успехи ребенка, его здоровье и отношения с семьей и друзьями? Выясните, сколько времени ваш ребенок проводит в интернете.

2. *Обратитесь за помощью*. Если у вашего ребенка проявляются серьезные признаки интернет-зависимости, проконсультируйтесь с педагогом. Навязчивое использование интернета может быть симптомом других проблем, таких как депрессия, раздражение или низкая самооценка.

3. *Не запрещайте интернет*. Для большинства детей он является важной частью их общественной жизни. Вместо этого установите *внутрисемейные правила использования интернета*. В них можно включить следующие ограничения: количество времени, которое ежедневно проводит в интернете ребенок; запрет на Сеть до выполнения домашней работы; ограничение на посещение чатов или просмотр материалов «для взрослых».

4. *Держите компьютер в открытом помещении*. Установите компьютер в общей комнате вашей квартиры, а не в спальне ребенка.

5. *Поддерживайте равновесие*. Пусть ребенок почаще играет с другими детьми на свежем воздухе.

6. *Помогайте ребенку участвовать в общении вне интернета*. Если ваш ребенок застенчив и испытывает неловкость при общении с ровесниками, почему бы не рассмотреть возможность специального тренинга? Поощряйте участие ребенка в тех видах деятельности, которые объединяют детей с одинаковыми интересами, например, моделирование кораблей или литературный кружок.

7. *Контролируйте своих детей*. Ознакомьтесь с программами, которые ограничивают использование интернета и осуществляют контроль над посещаемыми

сайтами. Однако помните, что сообразительный ребенок, если постарается, может и отключить эту службу. Поэтому ваша конечная цель – развитие у детей самоконтроля, дисциплины и ответственности.

8. *Предложите альтернативы*. Если вам кажется, что ваши дети интересуются только онлайновыми развлечениями, попробуйте предложить им автономный аналог одной из их любимых игр. Например, если ваш ребенок получает удовольствие от ролевых игр на тему фэнтези, предложите ему почитать книги соответствующей тематики.

Внутрисемейные правила использования интернета

Перед тем как дети начнут осваивать интернет, неплохо убедиться, что все понимают, что следует и что не следует делать в Сети. Можно написать кодекс поведения, которому все согласны следовать. Кроме того, можно составить правила пользования для каждого ребенка в семье в зависимости от возраста. Каждый подписывает свое соглашение, чтобы показать, что понимает правила и соглашается следовать им в интернете.

Ниже приведен образец. Его можно скопировать, пересмотреть для нужд именно вашей семьи и напечатать для личного использования. Семейные правила пользования Сетью можно прикрепить около каждого компьютера. Для напоминания.

Соглашение о кодексе поведения в Интернете

Я обязуюсь:

1. Обращаться к моим родителям, чтобы узнать правила пользования интернетом: куда мне можно заходить, что можно делать и как долго позволяется находиться в интернете (___ минут или ___ часов).
2. Никогда не выдавать без разрешения родителей личную информацию: домашний адрес, номер телефона, рабочий адрес или номер телефона родителей, номера кредитных карточек или название и расположение моей школы.
3. Всегда немедленно сообщать родителям, если я увижу или получу в интернете что-либо тревожащее меня или угрожающее мне; сюда входят сообщения электронной почты, сайты или даже содержимое обычной почты от друзей в интернете.
4. Никогда не соглашаться лично встретиться с человеком, с которым я познакомился в интернете, без разрешения родителей
5. Никогда не отправлять без разрешения родителей свои фотографии или фотографии членов семьи другим людям через интернет или обычной почтой.
6. Никогда никому, кроме своих родителей, не выдавать пароли интернета (даже лучшим друзьям).
7. Вести себя в интернете правильно и не делать ничего, что может обидеть или разозлить других людей или противоречит закону.
8. Никогда не загружать, не устанавливать и не копировать ничего с дисков или из интернета без должного разрешения.
9. Никогда не делать без разрешения родителей в интернете ничего, требующего платы.
10. Сообщить моим родителям мое регистрационное имя в интернете и имена в чате, перечисленные ниже:

_____

Имя (ребенок) _____ Дата _____

Родитель или опекун _____ Дата _____

Преступники в интернете: что можно сделать для снижения опасности

Пользуясь такими средствами связи, как чаты, электронная почта и система обмена мгновенными сообщениями, дети подвергаются опасности вступить в контакт со злоумышленниками. Анонимность общения в интернете способствует быстрому

возникновению доверительных и дружеских отношений. Преступники используют преимущества этой анонимности для завязывания отношений с неопытными молодыми людьми. Вы сможете защитить своих детей, если поймете возможную опасность общения через интернет и будете в курсе того, чем они занимаются в Сети.

Какие действия предпринимают интернет-преступники?

Преступники устанавливают контакты с детьми в чатах, при обмене мгновенными сообщениями, по электронной почте или на форумах. Для решения своих проблем многие подростки обращаются за поддержкой на конференции. Злоумышленники часто сами там обитают; они стараются прельстить свою цель вниманием, заботливостью, добротой и даже подарками, нередко затрачивая на эти усилия значительное время, деньги и энергию. Обычно они хорошо осведомлены о музыкальных новинках и современных увлечениях детей. Они выслушивают проблемы подростков и сочувствуют им. Но постепенно злоумышленники вносят в беседы оттенок сексуальности или демонстрируют материалы откровенно эротического содержания, пытаясь ослабить моральные запреты, сдерживающие молодых людей.

Некоторые преступники действуют быстрее других и сразу же заводят сексуальные беседы. Такой более прямолинейный подход может включать решительные действия или скрытое преследование жертвы. Преступники могут также рассматривать возможность встречи с детьми в реальной жизни.

Кому из молодых людей угрожает опасность?

Подростки являются наиболее уязвимой группой и подвергаются наибольшей опасности. Подростки стремятся исследовать свою сексуальность, уйти из-под контроля родителей и завязать новые отношения вне семьи. Несмотря на то что общение в интернете может быть полностью анонимным, они больше подвержены опасности, даже если до конца не осознают возможные последствия.

Наиболее уязвимые для злоумышленников молодые люди – это, как правило:

– новички в интернете, не знакомые с сетевым этикетом;

– недружелюбные пользователи;

– те, кто стремится попробовать все новое, связанное с острыми ощущениями;

– активно ищущие внимания и привязанности;

– бунтари;

– одинокие или брошенные;

– любопытные;

– испытывающие проблемы с сексуальной ориентацией;

– те, кого взрослые могут легко обмануть;

– те, кого привлекает субкультура, выходящая за рамки понимания их родителей.

Дети воображают, что они представляют себе всю опасность при общении с интернет-преступниками, однако на самом деле это далеко не так.

Что родители могут сделать для повышения безопасности?

Расскажите своим детям о существовании злоумышленников и о потенциальных опасностях интернета.

Маленьким детям не следует пользоваться чатами – слишком велика опасность. Только когда ваш ребенок подрастет, можно разрешить общаться там, где есть контроль над сообщениями (или, говоря компьютерным языком, «модерация»). Вообще имеет смысл, чтобы дети общались только в таких чатах.

Если ваши дети пользуются чатами, вам следует знать, какими именно и с кем они там беседуют. Лично посетите чат, чтобы проверить, на какие темы ведутся дискуссии.

Внушите детям, что никогда нельзя покидать общий чат. Многие сайты имеют «приватные комнаты», где пользователи могут вести беседы наедине – у администраторов нет возможности читать эти беседы. Такие «комнаты» часто называют «приватом».

Компьютер, подключенный к интернету, должен находиться в общей комнате; никогда не устанавливайте его в спальне ребенка. Преступнику гораздо труднее завязать отношения, если экран компьютера хорошо вами просматривается. Но сесть рядом с ребенком, когда он находится в Сети, необходимо в любом случае.

Пока дети маленькие, лучше, чтобы они пользовались общим электронным адресом семьи, а не своим собственным.

Объясните детям, что никогда не следует отвечать на мгновенные сообщения или письма по электронной почте, поступившие от незнакомцев. Если дети пользуются компьютерами в местах, находящихся вне вашего контроля, – общественной библиотеке, школе или дома у друзей – выясните, какие защитные средства там используются.

Если, несмотря на все меры предосторожности, ваши дети познакомились в интернете со злоумышленником, помните, что вся полнота ответственности всегда лежит на правонарушителе, поэтому не ругайте ребенка. Предпримите решительные действия для прекращения его дальнейших контактов с этим лицом.

Как ваши дети могут снизить риск стать жертвами преследований?

Дети могут предпринимать следующие меры предосторожности:

– никогда не скачивать изображения из неизвестного источника – они могут иметь откровенно сексуальный характер;

– использовать фильтры электронной почты;

– немедленно сообщать взрослым обо всех случаях в интернете, которые вызвали смущение или испуг;

– использовать нейтральное в половом отношении экранное имя, не содержащее сексуальных намеков и не выдающее никаких личных сведений;

– никогда и никому в интернете не сообщать информацию о себе (включая возраст и пол) или о семье; никогда не заполнять личные профили в Сети;

– прекращать любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вопросы личного характера или содержащие сексуальные намеки;

– следует повесить рядом с компьютером семейное соглашение, напоминающее детям о необходимости сохранять свою конфиденциальность в интернете.

Как узнать, не стал ли ваш ребенок потенциальной целью преступника?

Приведенные ниже признаки могут означать, что на вашего ребенка обратил внимание злоумышленник:

– ваш ребенок проводит много времени в интернете. Большинство детей, преследуемых интернет-преступниками, проводят большое количество времени в Сети, особенно в чатах; подчас закрывают дверь в свою комнату и скрывают, чем они занимаются во время работы на компьютере;

– в семейном компьютере появились порнографические материалы. Преступники нередко используют материалы откровенного содержания; в качестве предлога для начала сексуальных обсуждений преступники могут снабжать детей фотографиями, ссылками на соответствующие сайты и присылать сообщения эротической окраски. Для того чтобы внушить ребенку мысль о естественности сексуальных отношений между взрослыми и детьми, преступники могут использовать фотографии с

изображением детской порнографии. Вы должны отдавать себе отчет в том, что ваш ребенок может прятать порнографические файлы на дисках, особенно если другие члены семьи тоже пользуются компьютером;

– вашему ребенку звонят люди, которых вы не знаете, или он сам звонит по номерам (иногда в другие города), которые вам не знакомы. Установив в интернете контакт с вашим ребенком, некоторые злоумышленники могут попытаться вовлечь детей в секс по телефону или попытаться встретиться в реальной жизни. Если дети не решаются дать номер телефона, интернет-маньяк может сообщить им свой. Не разрешайте своему ребенку лично встречаться с незнакомцем без контроля с вашей стороны;

– ваш ребенок получает письма, подарки или посылки от неизвестного вам лица. Обычно преследователи посылают своим потенциальным жертвам письма, фотографии и подарки. Сексуальные извращенцы даже отправляют билеты на самолет, чтобы соблазнить ребенка личной встречей;

– ваш ребенок сторонится семьи и друзей и быстро выключает монитор компьютера или переключается на другое «окно», если в комнату входит взрослый. Интернет-преступники усердно вбивают клин между детьми и их семьями и часто преувеличивают небольшие неприятности в отношениях ребенка с близкими. Дети, подвергающиеся сексуальному преследованию, становятся замкнутыми и подавленными;

– ваш ребенок использует чью-то чужую учетную запись для выхода в интернет. Даже дети, не имеющие доступа в Сеть дома, могут встретить преследователя, выйдя в интернет у друзей или в каком-нибудь общественном месте, например, библиотеке. Иногда преступники предоставляют своим жертвам учетную запись, чтобы иметь возможность с ними общаться.

Что делать, если ваш ребенок стал потенциальной целью преступника?

Если ваш ребенок получает фотографии откровенно порнографического содержания или подвергается сексуальным домогательствам, обратитесь в местное отделение правоохранительных органов. Нужно сохранить всю информацию, включая адреса электронной почты, адреса сайтов и чатов, чтобы ознакомить с ней власть.

Проверьте компьютер на наличие порнографических файлов или каких-либо свидетельств об общении с сексуальной окраской – это настораживающие признаки.

Контролируйте доступ вашего ребенка ко всем средствам общения, работающим в режиме реального времени, таким, как чаты, мгновенные сообщения и электронная почта. Обычно интернет-преступники впервые встречают своих потенциальных жертв в чатах, а затем продолжают общаться с ними посредством электронной почты или мгновенных сообщений.