

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ



Федеральный закон Российской Федерации от 28 июля 2012 г. № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации»

КАК СДЕЛАТЬ ИНТЕРНЕТ ДЛЯ ДЕТЕЙ БОЛЕЕ БЕЗОПАСНЫМ

Интернет предоставляет детям и молодежи невероятные возможности для совершения открытий, общения и творчества. Тем не менее с использованием Интернета также связаны риски. Например, он представляет собой открытое окно в мир, который также принадлежит взрослым и содержит материалы, не подходящие для детей.

Как должны родители помочь детям снизить эти риски? Простого ответа не существует. Риски могут быть разными в зависимости от возраста и компьютерной грамотности ребенка.

Наиболее важным является обеспечение безопасности личной информации на собственном компьютере, что означает защиту от вирусов и обновление программного обеспечения. Что касается детей, повысить уровень защиты данных можно путем использования настроек фильтра и параметров фильтрации содержимого, которые доступны во многих программах.

Эта статья была написана сотрудниками компании Microsoft. В последнее время MS проводит активную образовательную политику, и многие ее учебные материалы заслуживают самого пристального внимания. Представляю вам очень любопытный документ, представляющий методическое пособие для родителей. Написанное просто и понятно, оно поднимает многие проблемы, с которыми сталкиваются многие родители.

Важно, чтобы компьютерное оборудование находилось в хорошем рабочем состоянии. Однако для детей и молодежи Интернет главным образом является социальной средой, в которой можно не только встречаться с друзьями, но и с незнакомцами. В Интернете пользователя могут обидеть, запугать или даже оскорбить. Лучшей защитой является руководство собственным здравым смыслом. Наиболее важной задачей является предупреждение детей об опасностях Интернета, чтобы они вели себя

осторожно. Кроме того, необходимо обсуждать с детьми все вопросы, которые могут у них возникнуть при использовании Интернета.

Использование Интернета является безопасным, если выполняются три основных правила:

ЗАЩИТИТЕ СВОЙ КОМПЬЮТЕР

Регулярно обновляйте операционную систему.

Используйте антивирусную программу.

Применяйте брандмауэр.

Создавайте резервные копии важных файлов.

Будьте осторожны при загрузке новых файлов.

ЗАЩИТИТЕ СЕБЯ В ИНТЕРНЕТЕ

С осторожностью разглашайте личную информацию. Думайте о том, с кем разговариваете. Помните, что в Интернете не вся информация надежна и не все пользователи откровенны.

СОБЛЮДАЙТЕ ПРАВИЛА

Закону необходимо подчиняться даже в Интернете.

При работе в Интернете не забывайте заботиться об остальных так же, как о себе.

ПОСТЕПЕННОЕ ЗАВОЕВАНИЕ ДОВЕРИЯ

Родители сталкиваются с одинаковыми трудностями как с Интернетом, так и с другими увлечениями детей. Родителям важно знать о намерениях своих детей и поддерживать их в этих действиях.

Дети могут не захотеть рассказывать о том, как они используют Интернет. Они могут быть против вмешательства родителей в процесс использования Интернета, особенно если они считают, что родители ограничат их в этом. Важно помнить о том, что Интернет является огромным ресурсом с большим объемом увлекательной и образовательной информации. Кроме того, важно не слишком остро реагировать или чрезмерно ограничивать детей в использовании Интернета. Чтобы дети могли извлечь самое лучшее из такого ресурса и для обеспечения их безопасности, необходимо осознавать все связанные с этим риски. Дети учатся, экспериментируя, путем проб и ошибок. Если вы сами увлекаетесь Интернетом и знакомы со всеми его аспектами, это очень поможет вам при обсуждении Интернета с детьми. Кроме того, вам будет проще выяснить, как ваш ребенок использует Интернет, и непрерывно вести диалог, который будет длиться до достижения детьми совершеннолетия.

Чем больше вы знаете о том, как ваш ребенок использует Интернет, тем проще будет определить и объяснить, что является приемлемым и безопасным. У ребенка могут быть превосходные навыки использования

Интернета, но жизненный опыт взрослых может оказаться бесценным при объяснении детям принципов поведения в виртуальном мире.

СОВЕТЫ

УСТАНОВИТЕ КОМПЬЮТЕР В ОБЩЕЙ ДЛЯ ВСЕЙ СЕМЬИ КОМНАТЕ

В этом случае разговор об Интернете и наблюдение за его использованием станет естественным в повседневной жизни. Обсуждение проблем может стать проще, если компьютер находится в общей комнате. Кроме того, Интернетом можно пользоваться вместе.

ОБСУЖДАЙТЕ ИНТЕРНЕТ

Проявляйте интерес к действиям ребенка и его/ее друзей как в Интернете, так и в реальной жизни. Расскажите ребенку о прекрасных и увлекательных вещах, которые возможны в Интернете, а также о трудностях, с которыми можно столкнуться. Обсудите с ребенком действия, которые необходимо предпринять, если чувствуется неловкость в какой-либо ситуации в Интернете.

УЗНАЙТЕ БОЛЬШЕ ОБ ИСПОЛЬЗОВАНИИ КОМПЬЮТЕРА

Если вы сами являетесь пользователем Интернета, вам будет проще определить правильную тактику для детей и помочь им найти в Интернете полезный материал.

ИСПОЛЬЗУЙТЕ ИНТЕРНЕТ ВМЕСТЕ

Найдите сайты, которые подходят для детей, или узнайте о способах поиска полезной информации: запланируйте совместную туристическую поездку, просмотрите образовательные сайты для помощи в школьных заданиях или найдите информацию об увлечениях детей. Просматривая веб-сайты в Интернете вместе, можно также помочь ребенку оценить значимость найденной информации. Можно добавить любимые сайты в папку «Избранное», чтобы совместно просмотренные ранее веб-сайты можно было открыть одним щелчком мыши.

ДОГОВАРИВАЙТЕСЬ С РЕБЕНКОМ О СПОСОБЕ И ВРЕМЕНИ ИСПОЛЬЗОВАНИЯ ИНТЕРНЕТА

Может оказаться полезным согласовать с ребенком время, которое он проводит за компьютером, а также список веб-сайтов, которые он может посещать. Это необходимо обсудить с детьми и прийти к определенному решению, которое всех устраивает.

ВНУТРЕННИЕ ПРАВИЛА ПО ИСПОЛЬЗОВАНИЮ ИНТЕРНЕТА

Существует один хороший способ свести к минимуму опасности Интернета, который заключается в установлении и согласовании с детьми некоторых правил. Общие правила являются отличным началом для разговора о безопасном использовании Интернета.

Время, проводимое за компьютером, необходимо ограничить по причинам, связанным со здоровьем.

Поместите компьютер, например, в гостиной. При использовании Интернета дошкольниками рекомендуется присутствие взрослого.

Доступ к Интернету для дошкольников необходимо ограничить до списка знакомых веб-сайтов, выбранных заранее. Более подготовленные дети могут найти знакомые сайты в меню «Избранное» обозревателя Интернета.

Самым безопасным решением является создание для ребенка персональной рабочей среды, в которой выбор сайтов ограничивается только указанными сайтами.

СОВЕТЫ РОДИТЕЛЕЙ

БЕЗОПАСНЫЕ ПАРОЛИ

Одним из способов является придумать известное предложение и взять из каждого слова первые буквы. Например, «Наш Сергей родился в 99», при этом с использованием английского алфавита получится пароль YChd99. Просто запомнить, сложно догадаться. Никогда не создавайте пароль, который может отгадать друг (например, кличка домашнего животного).

ФИЛЬТР ПОИСКА MSN

Детям известно, как использовать поисковые модули для информации, но им не обязательно знать, как избежать ссылок на все виды неуместного содержимого. Нами используется собственный фильтр поиска MSN, который исключает неуместные ссылки из результатов поиска.

Примечание. Не забудьте сохранить параметры при изменении уровня строгости фильтрации. Чтобы отключить фильтр, необходимо вернуться на страницу параметров поиска и выбрать умеренный уровень фильтрации или отключить ее полностью. Необходимо сохранить параметры, чтобы изменения вступили в силу.

В Интернете содержатся материалы, неуместные для детей. Большую часть таких материалов можно заблокировать с помощью ряда фильтров. Важно понимать, что такая технология не является единственным способом защиты детей от неуместных материалов в Интернете.

БЕЗОПАСНОЕ ПРОСТРАНСТВО

Самым безопасным способом путешествия по просторам Интернета для детей является создание безопасного пространства или области, в которой разрешен просмотр сайтов, одобренных доверенным взрослым человеком. Для разрешения детям доступа к определенным безопасным сайтам можно использовать параметры обозревателя. В этом случае, если ребенку необходимо посетить новый сайт, сначала необходимо добавить его адрес в список разрешенных сайтов. В операционной системе Windows XP можно легко создавать безопасные пространства.

Для ребенка необходимо создать персональную учетную запись пользователя в операционной системе. При этом для ребенка определяются права доступа и параметры обозревателя Интернета.

ПРОГРАММЫ ФИЛЬТРАЦИИ

Программы фильтрации предоставляют функции ограничения веб-сайтов на основе содержимого. Это означает, что программой блокируется доступ к сайтам, содержащим материалы, которые определены как опасные (порнография, насилие и т.д.).

Ограничение входящих контактов

С помощью технологии фильтров и блокировки можно ограничить список собеседников, с которым дети общаются через Интернет. Для получения более подробной информации см. страницы в разделах Использование электронной почты и Программы мгновенного обмена сообщениями.

ЖУРНАЛ ПРОСМОТРЕННЫХ ВЕБ-СТРАНИЦ

С помощью функции журнала просмотренных веб-страниц в обозревателе Интернета можно просмотреть веб-сайты, посещенные другими пользователями за последнее время (хотя журнал просмотренных веб-страниц легко удалить).

СОВЕТ

Что следует делать, если ребенок увидел в Интернете неприятные или неуместные материалы?

- Не реагируйте слишком остро: ребенок не должен чувствовать излишнего смущения, чтобы он мог свободно говорить о подобных случаях в будущем.
- Акцентируйте внимание ребенка на том, что это не его вина.
- Удалите любые следы, оставшиеся от неуместного материала, включая ссылки из кэш-памяти обозревателя, файлы cookie и журнал просмотренных веб-страниц.
- Поговорите с ребенком о том, как избежать подобных ситуаций в будущем, включая использование детских поисковых модулей и удаление сообщений электронной почты от неизвестных людей.

ОДНОРАНГОВЫЕ СЕТИ: ЗАГРУЗКА МУЗЫКИ, ИГР И ФИЛЬМОВ

Пользователь может загружать или копировать на компьютер файлы музыки, игр или фильмов. Такая загрузка обычно осуществляется с помощью специальных программ общего доступа к файлам (Kazaa, DirectConnect, BitTorrent и т.д.), в которых используется технология одноранговых сетей (p2p). Чтобы загрузить файлы из одноранговой сети, обычно требуется открыть общий доступ к файлам на компьютере для других пользователей сети. Во время этого процесса пользователь может случайно открыть доступ для копирования всех файлов в компьютере.

СОБЛЮДАЙТЕ АВТОРСКОЕ ПРАВО

Одноранговые сети иногда используются для распространения нелегальных копий музыки и фильмов, что является нарушением авторского права. Важно проверять достоверность сайта загрузки, который ребенок планирует использовать, для соблюдения авторского права. Необходимо руководствоваться принципом, что если за материал не взимается плата, он с большей вероятностью является незаконной загрузкой. При предоставлении общего доступа к файлам может снизиться скорость подключения к Интернету. В файлах, скопированных из неизвестных источников, могут также содержаться вирусы. В одноранговых сетях иногда может находиться незаконный материал или материал, неуместный для детей. Даже если имя файла указывает на то, что его содержимое уместно для детей, загружаемый файл мог быть назван неточно, поэтому имя файла не может гарантировать уместность его содержимого. В некоторых случаях имя файла может неточно отражать его содержимое.

Интерактивные обсуждения являются популярным способом общения среди детей. С помощью интерактивных чатов они всегда могут найти, с кем поговорить. Общение в Интернет-чатах может доставлять удовольствие и быть безопасным, только если пользователь способен обеспечить собственную безопасность. Прежде чем дети начнут общаться в Интернете, им необходимо рассказать о связанных с этим рисках и объяснить способ взаимодействия с другими пользователями, чтобы можно было защитить собственную личность. В этом разделе также содержится информация о различных типах общения, например об электронной почте, чате, IRC и программе мгновенного обмена сообщениями.

ПСЕВДОНИМЫ ОБЕСПЕЧИВАЮТ БЕЗОПАСНОСТЬ

В Интернете люди часто используют псевдонимы для защиты своей реальной личности. Общение под псевдонимом обеспечивает безопасность: с пользователем невозможно связаться, пока он сам не предоставит свою контактную информацию. Такая анонимность может, тем не менее, привести к неуместному поведению людей и к сквернословью. Дискуссионные группы часто могут состоять из группы зарегистрированных пользователей.

ПАРОЛИ ЯВЛЯЮТСЯ СЕКРЕТНЫМИ

Пользователям часто приходится создавать персональный профиль или учетную запись, чтобы принять участие в интерактивном обсуждении. Профиль представляет собой описание пользователя, например, идентификатор или псевдоним, используемый при обсуждении. В качестве защиты профиля обычно применяются пароли, которые позволяют предотвратить использование учетной записи другими людьми. Лучше всегда держать свой пароль в секрете.

НЕПРИКОСНОВЕННОСТЬ ЛИЧНОЙ ЖИЗНИ — ЧТО СЛЕДУЕТ И ЧТО НЕ СЛЕДУЕТ РАССКАЗЫВАТЬ О СЕБЕ?

В Интернет-чатах дети могут общаться с другими детьми и заводить новых друзей, что подразумевает обмен определенной личной информацией. Не следует разглашать в Интернете личную информацию, по которой можно установить личность ребенка, или контактную информацию (полное имя, почтовый адрес и номер телефона). Для защиты конфиденциальности в Интернете также необходимо понимать, каким образом может быть использована предоставляемая информация. Личность человека можно также установить, связав различные типы предоставленных данных (например, название школы, спортивного клуба, места проживания и т.д.).

Соблюдайте осторожность при разглашении контактных данных или другой личной информации. Любые отправляемые фотографии или раскрываемые незнакомцу личные сведения могут стать общедоступными в Интернете. Интерактивные дневники могут надолго стать доступными для прочтения широкой общественностью. После публикации в Интернете текста или фотографии их невозможно контролировать. Их можно легко скопировать во множество разных мест, и их полное удаление может оказаться невозможным.

Помните

Обсудите с детьми опасные последствия предоставления личной информации.

Личную информацию рекомендуется скрывать во многих различных ситуациях.

Пользователям никогда не следует сообщать пароли никому, даже давним друзьям. Кроме того, пароль необходимо регулярно менять.

Интернет является общественным местом. Перед публикацией любой информации или своих фотографий (а также фотографий других людей) следует помнить, что любой сможет получить доступ к этой информации. Чтобы выяснить, какая информация о вас доступна в Интернете, используйте поисковый модуль и в качестве поискового слова введите собственное имя.

Детям должна быть предоставлена возможность поговорить с родителями об отрицательном опыте, полученном в Интернете.

ЭЛЕКТРОННАЯ ПОЧТА

Электронная почта представляет собой широко распространенный способ отправки сообщений через Интернет, но важно использовать ее с осторожностью.

В папку входящих сообщений электронной почты может попадать спам, часто в форме рекламы, которая не предназначена специально для пользователя. Кроме риска получения вирусов через сообщения электронной

почты такого типа, в спаме может также содержаться неуместный материал или ссылки, которые непригодны для детей.

Через Интернет могут также распространяться анонимные сообщения электронной почты с целью оскорбления, запугивания или преследования.

Возможные действия

УСТАНОВКА ФИЛЬТРА СПАМА

Адрес электронной почты для ребенка рекомендуется получить у поставщика услуг Интернета, предоставляющего автоматическую защиту от вирусов и фильтрацию спама. Это помогает предотвратить получение большей части нежелательных сообщений.

РАЗРЕШЕНИЕ ТОЛЬКО ЗНАКОМЫХ ОТПРАВИТЕЛЕЙ

Вероятно, самый безопасный, хотя и очень ограниченный способ использования электронной почты — это настроить параметры так, чтобы ребенок получал сообщения только от указанных адресов. Многие программы электронной почты позволяют блокировать сообщения, отправляемые с определенных адресов электронной почты.

ПОЛУЧЕНИЕ АНОНИМНОГО АДРЕСА ЭЛЕКТРОННОЙ ПОЧТЫ

Адреса электронной почты часто выглядят как «имя.фамилия@домен.ru». Полное имя является личной информацией, которую не следует разглашать. Если ребенок хочет обмениваться сообщениями электронной почты с собеседниками из Интернета, лучшим способом является использование адреса электронной почты, в котором не раскрывается полное имя, например псевдоним01@домен.ru. В адресе электронной почты рекомендуется использовать цифры, поскольку в этом случае адрес будет сложнее «угадать», и, следовательно, на него будет приходить меньше спама. Не рекомендуется использовать этот же псевдоним в интерактивных чатах. От адреса электронной почты такого типа легче отказаться, если на него поступает большое число спама или других нежелательных сообщений. Широкополосная связь, как правило, включает несколько адресов электронной почты.

ЧАТ И IRC

ЧТО ТАКОЕ ЧАТ?

Чатом называется открытая дискуссионная группа в Интернете, в которой можно общаться с другими людьми в режиме реального времени, используя псевдоним. Чатам и группам чатов часто присваиваются названия на основе темы или возрастной группы. В обсуждении может участвовать множество пользователей, но часто также возможно личное общение между двумя пользователями. Общение в чатах предполагает собственный язык, этикет и даже культуру. Родителям было бы полезно знать о таких протоколах чатов. Рекомендуется выяснить это у своего ребенка.

ЧТО ТАКОЕ IRC?

С помощью IRC (система диалогового общения по Интернету) в Интернете можно проводить беседы в режиме реального времени. Эта система предоставляет более широкий выбор возможностей, чем простой чат. Для подключения к необходимым каналам (дискуссионным группам или комнатам) необходима отдельная программа — клиент IRC. С помощью IRC можно одновременно общаться на нескольких каналах, а также вести личные беседы между двумя людьми. В IRC применяются те же правила безопасного использования, что и для чатов. Для получения дополнительной информации об IRC посетите веб-сайт <http://www.neora.ru>.

ИНСТРУКЦИИ ПО БЕЗОПАСНОМУ ОБЩЕНИЮ В ЧАТАХ

Дети, которые общаются в чатах, должны знать, как делать это безопасным образом. Каждый должен помнить о следующих внутренних правилах чата.

1. Не доверяйте никому вашу личную информацию.
2. Сообщайте администратору чата о проявлениях оскорбительного поведения участников.
3. Если вам неприятно находиться в чате, покиньте его.
4. Если вам что-то не понравилось, обязательно расскажите об этом родителям.
5. Будьте тактичны по отношению к другим людям в чате.

ЧТО ТАКОЕ БЕЗОПАСНЫЙ ЧАТ?

Человек, с которым происходит общение, в значительной степени определяет, насколько безопасной и приятной для вас является атмосфера в чате. Как правило, степень безопасности чата, в котором общается ваш ребенок, можно определить по трем основным вопросам.

1. ПРЕДНАЗНАЧЕН ЛИ ЧАТ ДЛЯ ДЕТЕЙ?

В чатах, предназначенных для детей, вероятность неуместных тем или нежелательного контакта гораздо ниже.

2. ОСУЩЕСТВЛЯЕТСЯ ЛИ КОНТРОЛЬ ЗА ЧАТОМ?

Иногда в чатах работают добровольные модераторы, которые предотвращают случаи неуместного общения и могут заблокировать доступ в чат для хулиганов и других нарушителей порядка. Если контроль не осуществляется, в чате по крайней мере должна иметься кнопка для связи с администратором. Для детей предпочтительны контролируемые чаты; уровень безопасности также повышается, если беседы сохраняются.

3. ВОЗМОЖНО ЛИ ЗАБЛОКИРОВАТЬ ДОСТУП ДЛЯ ПОЛЬЗОВАТЕЛЕЙ?

Блокировка доступа подразумевает запрет размещения в чате сообщений от конкретного пользователя. После блокировки доступа для пользователя его сообщения больше не отображаются на экране.

ЛИЧНАЯ БЕСЕДА

При знакомстве с новым человеком в интерактивной дискуссионной группе, возможно, захочется перейти от общения в общественном чате к более личной беседе с глазу на глаз. Например, можно начать беседу в общей комнате чата, а затем перейти к общению с помощью программы мгновенного обмена сообщениями или переписке по электронной почте. При использовании этих средств можно по-прежнему обеспечить защиту своей личности путем использования псевдонима (например, псевдоним01@домен.ru). Кроме того, проще предоставить такой тип адреса на случай, если новым контактом окажется человек, с которым необходимо будет прекратить общение. Рекомендуется наставить детей, чтобы они отказывались от участия в личных интерактивных беседах с людьми, которых они не знают в жизни.

ВСТРЕЧА С СОБЕСЕДНИКАМИ ИЗ ИНТЕРНЕТА

Если ребенок общается в Интернете с новым человеком, возможно, ему/ей захочется лично встретиться с этим другом. Даже если дружба через Интернет поддерживалась в течение некоторого времени, эту встречу стоит воспринимать с осторожностью. Несмотря на то, что большинство встреч друзей по Интернету являются веселыми и безопасными мероприятиями, к сожалению, иногда они могут оставить неприятные впечатления. К счастью, случаи подобного рода крайне редки. Если встреча запланирована, настоятельно рекомендуется сопровождение ребенка родителем или другим взрослым, которому ребенок доверяет, а также проведение встречи в общественном месте. Лучше заранее согласовать с ребенком подход ко встрече с собеседниками из Интернета.

МГНОВЕННЫЙ ОБМЕН СООБЩЕНИЯМИ (MSN MESSENGER, ICQ И Т.Д.)

Так же, как и чаты, программы мгновенного обмена сообщениями позволяют общаться в режиме реального времени. Разница заключается в том, что пользователь может выбирать человека, с которым он хочет пообщаться. В программе отображаются те друзья, которые в настоящее время находятся в Интернете. Для участия в личной беседе можно пригласить одного или нескольких друзей. Кроме того, можно обмениваться файлами, например, фотографиями, музыкальными файлами или видеоклипами, играть в игры или совершать голосовые или видеовызовы.

Технология программ мгновенного обмена сообщениями подвержена тем же рискам, что и электронная почта с чатом. Пользователь может открыть вложение или ссылку, содержащую вирус, шпионскую программу или непригодный для детей материал. Общение в Интернете с человеком, которого вы знаете в жизни, гораздо безопаснее. Общение с помощью

программ мгновенного обмена сообщениями всегда является личным, и пользователь может контролировать не только то, с кем и как он разговаривает, но и время разговора.

Обсуждения можно сделать еще более безопасными путем настройки параметров программы мгновенного обмена сообщениями, как это описано ниже.

При первом использовании программы необходимо указать профиль пользователя. Не вводите данные, по которым можно установить вашу личность, поскольку профиль будет доступен всем участникам чата. Для многих интерактивных дискуссионных групп и интерактивных игр потребуется также заполнить профиль пользователя, поэтому в этих областях следует придерживаться этих же правил.

ВЫБОР ЛЮДЕЙ ДЛЯ ОБЩЕНИЯ

Безопаснее всего общаться с людьми, которые уже знакомы пользователю в реальной жизни. Тем не менее потенциально любой человек может отправлять сообщения вашему ребенку. В таких программах используется список контактов, позволяющий добавлять имена людей, с которыми пользователь желает обмениваться сообщениями. Чтобы ребенок не получал сообщений от незнакомцев, можно настроить параметры программы на блокировку контактов, отсутствующих в списке.

Попросите ребенка показать его список контактов и сказать, с кем он знаком в жизни и с кем он познакомился в Интернете. Это даст родителям более широкое представление о том, с кем ребенок общается в Интернете.

СОХРАНЕНИЕ БЕСЕД

Интерактивные беседы можно сохранять. Если другие участники чата видят, что сообщения сохраняются, это может повысить уровень безопасности ребенка. Если люди общаются в Интернете и им известно, что сообщения сохраняются, это часто делает их более осторожными во время интерактивного обсуждения. Программу можно настроить на сохранение только одной беседы или всех бесед автоматически.

МГНОВЕННЫЙ ОБМЕН СООБЩЕНИЯМИ (IM) — РАЗВЛЕЧЕНИЕ ДЛЯ ВСЕЙ СЕМЬИ

Мгновенный обмен сообщениями предназначен не только для детей и молодежи: во многих компаниях также используются программы мгновенного обмена сообщениями для внутренней связи. Например, если ребенок подключается к Интернету после школы, когда родители находятся на работе, можно обмениваться сообщениями и экономить затраты на телефон. Кроме того, можно отслеживать использование Интернета ребенком, поскольку в программе IM отображается время подключения.

ПРАВА ДЕТЕЙ В ИНТЕРНЕТЕ

ЗАПУГИВАНИЕ В ИНТЕРНЕТЕ

Интернет открывает новые возможности для оскорбительного поведения. Люди могут публиковать в Интернете слухи, фотографии или другую личную информацию, либо отправлять злоумышленные сообщения как анонимно, так и от чужого имени. Сообщения SMS и камералоны открывают новые возможности не только для развлечения, но и для эксплуатации. Запугивание в школе обычно заканчивается вместе с занятиями, но в Интернете обидчик может настигнуть свою жертву в любое время. Кроме того, у этих обидчиков имеется список пользователей, которых они могут запугивать в Интернете. Если ребенку нравится общаться через Интернет, такие риски необходимо обсудить заранее и ему необходимо дать совет относительно действий, которые следует предпринять при причинении беспокойства.

Это является важным по следующим причинам:

Запугивание в Интернете часто происходит в отсутствии взрослых.

Дети часто полагают, что если сообщить об этом родителям, это только усугубит ситуацию.

Анонимность и низкая вероятность быть наказанным приводит к тому, что люди начинают делать то, чего они не сделают в других обстоятельствах (например, могут сказать человеку то, чего они не скажут при личном общении).

Запугивание в Интернете легко осуществимо с технической точки зрения. Для отправки злонамеренного сообщения или публикации оскорбительного текста, доступного широкой аудитории, требуется несколько щелчков мышью.

СОВЕТ

Даже если ребенок не сталкивался с оскорблениями в Интернете, рекомендуется обсудить с ним/ней следующие вопросы:

Не распространяйте контактную или личную информацию, например, фотографии, без тщательного обдумывания возможных последствий. Интерактивная дружба может закончиться. Когда это произойдет, личная информация может быть отправлена злоумышленникам.

В Интернете каждый человек имеет право на уважительное отношение.

Чат, клиент электронной почты или компьютер можно закрыть или выключить в любое время.

Детям должна быть предоставлена возможность поговорить с родителями об отрицательном опыте.

ПОМНИТЕ

На Интернет распространяются те же нормативы и законы, что и в реальной жизни. В Интернете запрещается клеветать или оскорблять других

пользователей. Это может рассматриваться как пасквиль, за который пользователь может подвергнуться наказанию и ответственности за ущерб. Некоторые действия, для которых потребовалось несколько щелчков мыши, очень сложно отменить, и дети могут не понять, насколько серьезной может стать ситуация.

Помните, что анонимных пользователей часто можно отследить. Тем не менее, полиция не будет предпринимать никаких действий при отсутствии повода подозревать кого-либо в преступлении.

ЕСЛИ РЕБЕНОК ПОЛУЧАЕТ ЗЛОНАМЕРЕННЫЕ СООБЩЕНИЯ ПО ЭЛЕКТРОННОЙ ПОЧТЕ ИЛИ SMS:

Скажите ребенку, что не следует открывать такие сообщения или сообщения от полностью незнакомых людей.

Не следует отвечать на злонамеренные сообщения. Тем не менее, эти сообщения следует сохранять на случай, если в такую же ситуацию попадет другой человек.

Если выяснится, что отправитель учится в одной школе с ребенком, обратитесь в администрацию школы.

Если оскорбление не прекращается, можно изменить адрес электронной почты или номер телефона ребенка.

ДОПОЛНИТЕЛЬНЫЕ ПРАВИЛА:

Злонамеренные сообщения можно сохранять для последующих действий.

Кроме того, можно настроить параметры программы работы с электронной почтой так, чтобы сообщения от определенного отправителя поступали в отдельную папку. В этом случае ребенку не придется их читать.

Если известен адрес электронной почты отправителя, можно отправить копию злонамеренного сообщения поставщику услуг Интернета и попросить его удалить этот адрес электронной почты.

Если адрес электронной почты отправителя неизвестен, обратитесь за помощью к поставщику услуг Интернета.

ПРИ ОБНАРУЖЕНИИ ОПУБЛИКОВАННЫХ В ИНТЕРНЕТЕ ОСКОРБИТЕЛЬНЫХ ТЕКСТОВ О РЕБЕНКЕ ИЛИ ЕГО ФОТОГРАФИЙ:

Сохраните все страницы, на которых был найден этот материал, для последующих действий.

Если по сайту или его адресу можно определить поставщика услуг, необходимо связаться с ним. Поставщик услуг может удалить текст и, вероятно, раскрыть личность автора.

Кроме того, можно попросить собственного оператора Интернета связаться с администратором данного сайта и запросить удаление материалов.

Если оскорбление очень серьезное и является преступлением, обратитесь в полицию.

ДЕТИ И МАРКЕТИНГ В ИНТЕРНЕТЕ

Интернет является для рекламодателей эффективным способом продвижения рекламы для детей и молодежи. Многие товары, которые нравятся детям, продаются через Интернет.

Торговля, нацеленная на детей, регулируется

Торговля, нацеленная на детей и подростков, осуждается и регулируется более строго, чем торговля, нацеленная на взрослых, поскольку несовершеннолетние больше подвержены влиянию рекламы. В Федеральном законе РФ «О рекламе» (<http://www.gdezakon.ru/fz/rekl>) содержится ряд требований к торговле, нацеленной на несовершеннолетних. Ниже представлены некоторые из пунктов:

Не допускается размещение рекламы в учебниках, предназначенных для обучения несовершеннолетних

Не допускается дискредитация родителей и воспитателей

Не допускается создание у несовершеннолетних искаженного представления о доступности товара.

ВОЗМОЖНЫЕ ДЕЙСТВИЯ:

Используйте Интернет вместе с ребенком и учите его/ее выявлять рекламу и ее цели.

Сообщайте в Потребительское агентство или поставщику услуг об обнаружении любой неуместной рекламы.

ЗАЩИТА ДЕТЕЙ ОТ ПРЯМОГО МАРКЕТИНГА

Прямой маркетинг через сообщения электронной почты или SMS разрешен только с предварительного согласия человека. Например, если ребенок предоставляет личную информацию при участии в соревновании в Интернете, он/она может по невнимательности дать согласие на прямой маркетинг.

Платные услуги и совершение покупок детьми в Интернете

Любые покупки, совершаемые в Интернете или по мобильному телефону, должны осуществляться взрослым, либо осуществляться с его разрешения.

СОВЕТЫ:

- Согласуйте с ребенком правила совершения покупок в Интернете.
- В сотрудничестве с оператором установите необходимые блокировки для телефона, сообщений SMS или ограничения расходов в мобильном телефоне ребенка.
- Сообщайте в отделы управления «К» БСТМ МВД РФ Вашего региона или поставщику услуг о любых неуместных веб-сайтах.
- Создайте семейный адрес электронной почты для использования вами и детьми при приобретении товаров через Интернет.

ЛИЧНАЯ ИНФОРМАЦИЯ И ФОТОГРАФИИ ДЕТЕЙ В ИНТЕРНЕТЕ

В нашей семье мы взяли за правило, что один из родителей всегда проверяет надежность услуг Интернета, прежде чем дети смогут передать информацию на сайт. Обычно не требуется вводить всю запрашиваемую информацию, поэтому мы рекомендуем детям предоставлять только обязательные сведения.

На многих веб-сайтах пользователей просят зарегистрироваться или другим образом предоставить личную информацию для получения вознаграждений, например, доступа к услуге, участия в лотерее, получения бесплатных товаров или возможности участия в дискуссионной группе. Коммерческие организации могут собрать контактную информацию о детях и подростках в целях маркетинга, но перед осуществлением маркетинговой деятельности они должны получить согласие на законных основаниях.

Тем не менее, администраторы веб-сайтов могут не всегда сохранять конфиденциальность личной информации, даже если эти сведения защищены Законом об охране информации. Научите детей быть осторожными при предоставлении личной информации.

СОВЕТЫ

Договоритесь с ребенком о подходе. Зачастую бывает полезным договориться с ребенком о принципах предоставления личной информации в Интернете. Если ребенку разрешается предоставление подобной информации, необходимо знать о надежности сайтов, на которых предоставлялись сведения.

Ознакомьтесь с политикой защиты конфиденциальной информации. Мы советуем каждый раз проверять, прилагается ли к используемой службе соответствующая политика защиты конфиденциальной информации, в которой должен объясняться способ использования личной информации, время и цели ее использования.