ОПАСНОСТИ И ПРАВИЛА БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ

Смежная специальность современного родителя – это Интернет-Ангел хранитель.

ПРЕСТУПНИКИ В ИНТЕРНЕТЕ: ЧТО МОЖНО СДЕЛАТЬ ДЛЯ СНИЖЕНИЯ ОПАСНОСТИ

Пользуясь возможностями Интернета, 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.

ДЕЙСТВИЯ, КОТОРЫЕ ПРЕДПРИНИМАЮТ ПРЕСТУПНИКИ В ИНТЕРНЕТЕ. Преступники преимущественно 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 привлечь подростка своим 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 свои беседы оттенок сексуальности или демонстрируют материалы откровенно эротического содержания, пытаясь ослабить моральные запреты, сдерживающие молодых людей. Некоторые преступники могут действовать быстрее других и сразу же заводить сексуальные беседы. Преступники могут также оценивать возможность встречи с детьми в реальной жизни.

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, сидя за компьютером.

В семейном компьютере появились материалы откровенного содержания. В качестве предлога для начала сексуальных обсуждений злоумышленники 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. Имейте в виду, что ваш ребенок может прятать порнографические файлы на дисках, особенно если другие члены семьи пользуются тем же компьютером.

Вашему ребенку звонят люди, которых вы не знаете, или он сам звонит по номерам, которые вам незнакомы. 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, злоумышленник 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. В других странах они порой 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. Кроме того, 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? Регулярно проверяйте компьютер на наличие материалов откровенного характера 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.

Не вините детей. Если, несмотря на все меры предосторожности, ваши дети познакомились в Интернете со злоумышленником, вся полнота ответственности всегда лежит на правонарушителе. Предпримите решительные действия для прекращения дальнейших контактов ребенка с этим лицом.

Если ваш ребенок получает фотографии откровенного характера или подвергается сексуальным домогательствам, сохраните всю имеющуюся информацию, включая адреса электронной почты, адреса сайтов и чатов, чтобы иметь возможность ознакомить с ней представителей власти.

ЧТО ДЕТИ ДОЛЖНЫ ЗНАТЬ О ВРЕДОНОСНЫХ И НЕЖЕЛАТЕЛЬНЫХ ПРОГРАММАХ В ИНТЕРНЕТЕ

К вредоносным программам относятся вирусы, черви и «троянские кони» – это компьютерные программы, которые могут нанести вред вашему семейному компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом и даже использовать ваш компьютер для распространения своих копий на компьютеры ваших друзей, родственников, коллег и по всей остальной глобальной Сети. Но хорошо то, что, проявив здравый смысл и предприняв меры по предотвращению опасности, а также объяснив эти опасности своим детям, ваша семья с меньшей вероятностью станет жертвой подобных угроз.

ЧТО ТАКОЕ ВИРУС? Объясните детям, что вирусы – это программы, которые мешают нормальной работе компьютера, перезаписывают, повреждают или удаляют данные. Они также распространяются между компьютерами в Сети и через Интернет, часто замедляя их работу и вызывая другие неполадки.

Так же как вирусы человека различаются по степени опасности (от вируса Эбола до вируса 24-часового гриппа), так и компьютерные вирусы могут быть как слегка неприятными, так и безусловно разрушительными. Однако у них есть и хорошая сторона: настоящий вирус не может распространяться без участия человека. Для продвижения вируса кто-то должен распространить файл или отправить электронное письмо.
Более сложные вирусы, например черви, могут автоматически самовоспроизводиться на других компьютерах, устанавливая контроль над программами (например, приложениями электронной почты). Некоторые вирусы – «троянские кони» (названные так в честь легендарного Троянского коня) – выглядят как полезные программы и обманом убеждают пользователей загрузить их. Отдельные «троянские кони» способны даже работать как полезная программа, одновременно нанося вред системе или другим компьютерам, подключенным к Сети.

Иметь представление о разновидностях вирусов и принципах их функционирования необходимо, но гораздо важнее регулярно устанавливать на компьютере последние обновления безопасности и антивирусные средства.

ЧТО ТАКОЕ НЕЖЕЛАТЕЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ? Объясните детям, что под выражением «нежелательное программное обеспечение» понимаются программы, которые выполняют на компьютере некие задачи без вашего согласия. Они могут показывать рекламные сообщения, объявления или собирать личные данные о вас и вашей семье.

КАК МОЖНО ОПРЕДЕЛИТЬ, ЧТО ВАШ КОМПЬЮТЕР ЗАРАЖЕН? Ваш компьютер может начать работать медленнее или прекращать работать и перезагружаться каждые несколько минут. Иногда вирус атакует файлы, необходимые для запуска компьютера. В подобном случае вы можете, нажав кнопку запуска, обнаружить, что смотрите на пустой экран.

Все эти симптомы являются типичными признаками заражения компьютера вирусом, хотя они могут вызываться также проблемами в аппаратной части или программном обеспечении, не имеющими ничего общего с вирусным заражением.

Совет: Помните, что, открыв и запустив зараженный файл, вы можете не сразу узнать, что получили вредоносную программу, так как вирусы часто начинают свою разрушительную работу не сразу.

Пусть дети будут внимательны к сообщениям о том, что они отправили электронное письмо, содержащее вирус. Это может значить, что вирус указал ваш электронный адрес в качестве отправителя зараженного письма. Это необязательно означает, что на вашем компьютере есть вирус. Некоторые вирусы умеют фальсифицировать электронные адреса.

Microsoft по адресу http://www.microsoft.com/rus/athome/security/downloads/default.mspx.

ЧТО ДЕТИ ДОЛЖНЫ ЗНАТЬ ОБ ИНТЕРНЕТ-МОШЕННИЧЕСТВЕ И ХИЩЕНИЯХ ДАННЫХ КРЕДИТНОЙ КАРТЫ

В России мошенничество с помощью Интернета или хищения данных кредитной карты еще не стали очень широко распространены. Однако мы можем стоять на пороге этого явления, и нужно сделать так, чтобы оно не застало нас врасплох.

В ЧЕМ СОСТОИТ МОШЕННИЧЕСТВО? Среди Интернет-мошенничеств широкое распространение получила применяемая хакерами техника «phishing», состоящая в том, что в фальшивое электронное письмо включается ссылка, ведущая на популярный узел, но в действительности она приводит пользователя на мошеннический узел, который выглядит точно так же, как официальный. Убедив пользователя в том, что он находится на официальном узле, хакеры пытаются склонить его к вводу паролей, номеров кредитных карт и другой секретной информации, которая потом может и будет использована с ущербом для пользователя.

Кроме того, если вы сами или ваши дети пользуетесь кредитной картой для оплаты товаров и услуг через Интернет, по телефону или даже лично в соседнем магазине, вы уязвимы для мошенников. При любой операции оплаты с использованием кредитной карты компании должны проверить информацию о счете, прежде чем предоставить товары или услуги. Данные о кредитных картах хранятся на крупных серверах. К сожалению, хакеры могут взломать такую систему и завладеть информацией, чтобы воспользоваться ею в корыстных целях, например, оплачивать свои счета, используя деньги с вашей карты.

СНИЖЕНИЕ РИСКА ХИЩЕНИЯ ЛИЧНЫХ ДАННЫХ. Посещая веб-сайты, нужно самостоятельно набирать в обозревателе адрес веб-сайта или пользоваться ссылкой из «Избранного» (Favorites); никогда не нужно щелкать на ссылку, содержащуюся в подозрительном электронном письме.

Нужно как можно быстрее обратиться к настоящим сотрудникам организации, если получилось так, что конфиденциальная информация была предоставлена вами или вашими детьми неизвестным лицам, выдающим себя за сотрудников той или иной компании либо организации. При немедленном обращении компания может уменьшить ущерб, нанесенный вашей семье и другим лицам.

Контролируйте списание средств с ваших кредитных или лицевых счетов. Для этого можно использовать, например, услугу информирования об операциях со счетов по SMS, которые предоставляют в том числе и многие банки в России.

ЧТО ДЕЛАТЬ В СЛУЧАЕ ХИЩЕНИЯ ЛИЧНЫХ ДАННЫХ? Если вы подозреваете, что ваши личные данные украдены, немедленно принимайте меры:

- Измените пароли.
- Поставьте в известность отдел обслуживания клиентов соответствующих организаций.
- Поставьте в известность свой банк или финансовую организацию, если необходимо, то закройте или временно заблокируйте ваши счета.
- Запросите отчет о финансовых операциях и проверьте их корректность, о выявленных расхождениях поставьте в известность вашу финансовую организацию.
- Записывайте и сохраняйте абсолютно все.
- После выполнения всех действий всегда делайте копии документов.

В виртуальном мире есть свои правила Интернет-гигиены.

АЗАРТНЫЕ ИГРЫ В ИНТЕРНЕТЕ: КАК ПРЕДОСТЕРЕЧЬ ДЕТЕЙ?

В ЧЕМ СОСТОИТ ОТЛИЧИЕ МЕЖДУ ИГРОВЫМИ САЙТАМИ И САЙТАМИ С АЗАРТНЫМИ ИГРАМИ. Множество детей обожают искать развлечения (например, игры) в Интернете. Иногда при поиске нового игрового сайта они могут попасть на карточный сервер. Большинство игр и развлечений для несовершеннолетних вполне законны, однако им нельзя играть в азартные игры на деньги.

Разница между игровыми сайтами и сайтами с азартными играми состоит в том, что на игровых сайтах обычно содержатся настольные и словесные игры, аркады и головоломки с системой начисления очков. Здесь не тратятся деньги: ни настоящие, ни игровые. Сайты с азартными играми могут допускать, что люди выигрывают или проигрывают игровые деньги. Сайты с играми на деньги обычно содержат игры, связанные с выигрышем или проигрышем настоящих денег.

КАК ПРЕДОСТЕРЕЧЬ ДЕТЕЙ ОТ ИГР НА ДЕНЬГИ? Родители должны решить, во что можно играть их детям. Обсудите жанр игр (скажем, только бильярд, стратегии и шахматы) и количество участников (можно ведь играть и одному).

Напоминайте детям, что им нельзя играть на деньги. Предложите им играть в не менее увлекательные игры, но которые не предполагают использование наличных или безналичных проигрышей/выигрышей.

Помогите детям понять механизм таких игр. Ведь в основном подобные развлечения используются создателями для получения прибыли. Игроки больше теряют деньги, нежели выигрывают.

Не позволяйте детям использовать номера ваших кредитных карт в Интернете. Держите их в недоступном для детей месте. В сетевых играх на деньги они обычно требуются. Дети могут ненароком влезть в долги.

Объясните, что к играм на деньги можно пристраститься. Всегда есть опасность приобретения зависимости. Это как болезнь. Особенно если есть кредитная карта и положительный баланс на ней; человек может играть, пока не истратит все до конца.

Контролируйте поведение своих детей в Интернете. Следите за тем, какие сайты посещают ваши дети и что они делают в Интернете.

Бесплатный сыр бывает и в Интернет-мышеловках.

ИНТЕРНЕТ-ЗАВИСИМОСТЬ: ЕСТЬ ЛИ ОНА У ВАШИХ ДЕТЕЙ?

То, что дети проводят в Интернете слишком много времени, огорчает большинство родителей. Сначала взрослые приветствовали появление Сети, полагая, что она – безграничный источник новых знаний. Вскоре выяснилось, что подростки не столько пользуются Интернетом для выполнения домашних заданий или поиска полезной информации, сколько общаются в чатах и играют в онлайновые игры.

Поддержание в жизни детей разумного равновесия между развлечениями и другими занятиями всегда было испытанием для родителей; Интернет сделал это еще более трудной задачей. Общение в Интернете и интерактивные игры могут настолько затягивать детей, что они часто теряют ощущение времени. Несколько советов ниже помогут вашим детям не впасть в Интернет-зависимость.

СОВЕТЫ ПО ПРОФИЛАКТИКЕ ИНТЕРНЕТ-ЗАВИСИМОСТИ. Обратите внимание на психологические особенности вашего ребенка. Социально дезадаптированные дети имеют повышенную вероятность к приобретению Интернет-зависимости. Причина в том, что Интернет позволяет оставаться анонимным, не бояться осуждения (если что-то сделал неправильно, всегда можно поменять имя и начать все заново), предоставляет гораздо более широкий выбор возможностей к общению, чем реальный мир. В Интернете ребенку гораздо легче выстроить свой виртуальный мир, пребывание в котором ему будет

комфортным. Поэтому, если у ребенка что-то не получается в реальном мире, он будет стремиться к пребыванию там, где ему комфортно. С другой стороны, Интернет может помочь застенчивому ребенку стать более общительным, найти ту среду общения, которая более полно соответствует его уровню развития, и в результате повысить его самооценку. Если ваш ребенок в жизни замкнут, застенчив или склонен к унынию, вам необходимо внимательно следить за его отношением к Интернету, с тем чтобы предотвратить его превращение из средства раскрытия личности ребенка в плохо контролируемую страсть.

Следите за симптомами проявления Интернет-зависимости. Она проявляется в том, что дети до такой степени предпочитают жизнь в Интернете, что фактически начинают отказываться от своей реальной жизни, проводя в виртуальной реальности большую часть своего времени. Интернет-зависимый ребенок чаще всего тих и замкнут, он ждет не дождется, когда можно будет подключиться к Интернету, ему тяжело выйти из него, он впадает в депрессию или становится раздражительным, если на несколько дней его отлучили от Интернета. Интернет-независимый ребенок легко может переключиться на другой канал общения, выйти из Интернета, когда в этом возникает необходимость, он всегда четко различает, где он сейчас общается – в Сети или нет. Спросите себя: оказывает ли времяпровождение в Сети влияние на школьные успехи вашего ребенка, его здоровье и отношения с семьей и друзьями? Выясните, сколько времени ваш ребенок проводит в Интернете.

Обратитесь за помощью к специалистам. Если у вашего ребенка проявляются серьезные признаки Интернет-зависимости, проконсультируйтесь с педагогом или психологом. Навязчивое использование Интернета может быть симптомом других проблем, таких, как депрессия, раздражение или низкая самооценка. И когда эти проблемы будут решены, зависимость от Интернета может пройти сама собой.

Не запрещайте Интернет. Для большинства детей он является важной частью их общественной жизни. Вместо этого установите «Внутрисемейные правила использования Интернета» (см с. 34 данного издания) . 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».

Поддерживайте равновесие. Пусть ребенок почаще играет с другими детьми на свежем воздухе. Мотивируйте его на такое общение.

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, судомодельный или литературный кружок.

Контролируйте своих детей. Существуют программы, которые ограничивают использование Интернета и осуществляют контроль за тем, какие сайты посещаются, например MSN® Premium. Однако сообразительный ребенок, если постарается, может и отключить эту службу. Поэтому ваша конечная цель – развитие у детей самоконтроля, дисциплины и ответственности.

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 той же тематики.

Следите за достижением равновесия у вашего ребенка между временем, проводимым в Интернете и вне его.

ОНЛАЙНОВОЕ ПИРАТСТВО У СЕБЯ ДОМА: КАК ПРЕДОТВРАТИТЬ?

Онлайновое пиратство – это незаконное копирование и распространение (как для деловых, так и для личных целей) материалов, защищенных авторским правом – например, музыки, фильмов, игр или программ – без разрешения правообладателя.

СНИЖЕНИЕ РИСКА ПИРАТСТВА У СЕБЯ ДОМА. Предупредите детей о возможных опасностях. Пиратство, по сути, обычное воровство, и, скорее всего, вы вряд ли собираетесь поощрять воровство в своей семье. И чем раньше ваши дети это поймут, тем лучше. Однако не всегда бывает достаточно сказать детям о том, что какая-то деятельность – это плохо. В таком случае попробуйте просто поговорить с ними о возможных последствиях. Объясните вашим детям, что если они незаконно скачивают файлы, то ваш компьютер рискует стать уязвимым для вирусов или программ-шпионов.

Совет: Внушите своим детям, что нельзя незаконно скачивать или распространять фильмы, музыкальные файлы и программы.

Объясните детям, что подлинные (лицензионные) продукты всегда выгоднее и надежнее пиратской продукции. Официальный производитель несет ответственность за то, что он вам продает, он дорожит своей репутацией, чего нельзя сказать о компаниях – распространителях пиратских продуктов, которые преследуют только одну цель – обогатиться и за счет потребителя, и за счет производителя. Лицензионный пользователь программного обеспечения всегда может рассчитывать на консультационную и другую сервисную поддержку производителя, о чем пользователь пиратской копии может даже не вспоминать. Кроме того, приобретая лицензионный продукт, потребитель поддерживает развитие этого продукта, выход новых, более совершенных и удобных версий. Ведь в развитие продукта свой доход инвестирует только официальный производитель.

Научите своих детей законным методам скачивания. В Интернете существует множество мест, где вы и ваши дети можете скачать программы, фильмы, игры и музыку бесплатно или за небольшую цену. Например, сайт MSN Music предлагает более миллиона записей от разных студий.

Обсудите с детьми допустимые траты на музыкальные записи или игры, чтобы у молодого поколения не было соблазна для незаконного скачивания.

БЕЗОПАСНОЕ ОБЩЕНИЕ ДЕТЕЙ В ИНТЕРНЕТЕ

Интернет предоставляет несколько форм общения между участниками, которые любят использовать дети и подростки: чаты, системы обмена мгновенными сообщениями, блоги или Интернет-дневники.

В ЧЕМ СОСТОИТ ОБЩЕНИЕ ДЕТЕЙ В ЧАТАХ И СИСТЕМАХ ОБМЕНА МГНОВЕННЫМИ СООБЩЕНИЯМ? Возможно, вы слышали о чатах, в которых люди встречаются для обмена сообщениями на определенную тему. Может быть, вы даже сами там общались. Комнаты чата, в которых происходит общение, представляют собой виртуальные помещения в Сети, в которых люди могут набирать сообщения, почти мгновенно появляющиеся на экранах компьютеров других участников. Чаты обычно являются анонимными, поскольку участники пользуются псевдонимами.

В Интернете существует множество чатов различной направленности. В них предоставляется потрясающая возможность обсуждать разные темы с людьми со всего мира. Чаты очень популярны среди детей, и, к сожалению, преступникам это известно. Поэтому эта форма общения представляет особенную опасность для детей и подростков.

Многие люди, говоря об общении в системе обмена мгновенными сообщениями, называют это общением в чате, однако все же существует небольшая разница. Первая обычно используется для беседы между двумя собеседниками, в то время как в чате идет разговор с группой людей, но основные правила безопасности остаются одними и теми же.

КАК СДЕЛАТЬ ОБЩЕНИЕ В ИНТЕРНЕТЕ КОМФОРТНЫМ? Контролируйте использование чата вашим ребенком. Помните о том, что дети могут участвовать в чатах, расположенных на сайтах, при помощи программ поддержки чатов, сотовых телефонов и даже некоторых онлайновых игр.

Добейтесь того, чтобы дети никогда не сообщали в чатах свои личные данные. Так, при выборе псевдонима необходимо выбирать имя, не выдающее личные данные детей. Например, вместо псевдонима DetroitSue можно использовать SassySue. Следует настоять на том, чтобы дети не посылали своих фотографий тем, с кем они познакомились в чате.

Дети должны знать, что они всегда могут обратиться к вам за советом или помощью. Предупредите ребенка о том, что, если что-либо в чате вызовет у него чувство дискомфорта, необходимо немедленно его покинуть и сообщить о происшедшем кому-нибудь из взрослых. Пусть дети всегда сообщают вам об участниках чата, которые предлагают им встретиться в приватных комнатах чата.

У детей должно быть настороженное отношение к попыткам собеседников перевести общение из виртуальной плоскости в реальную. Им никогда нельзя соглашаться на личную встречу с незнакомыми людьми, с которыми они познакомились в Интернете.

Скажите детям, чтобы они посещали только модерируемые чаты. Перед тем как вступить в беседу, пусть ознакомятся с положениями и условиями участия в чате, правилах поведения и положением о конфиденциальности.

ИНТЕРНЕТ-ДНЕВНИКИ: ОСНОВЫ БЕЗОПАСНОГО ВЕДЕНИЯ

Увлечение веб-журналами (или, иначе говоря, блогами) распространяется со скоростью пожара, особенно среди подростков, которые порой ведут Интернет-дневники без ведома взрослых.

Последние исследования показывают, что сегодня примерно половина всех веб-журналов принадлежат подросткам. При этом двое из трех раскрывают свой возраст; трое из пяти публикуют сведения о месте проживания и контактную информацию, а каждый пятый сообщает свое полное имя. Не секрет, что подробное раскрытие личных данных потенциально опасно.

При этом все больше молодых пользователей создают собственные дневники, и каждый стремится привлечь как можно больше внимания аудитории. Иногда это приводит к тому, что дети размещают в блогах такой неуместный материал, как провокационные фотографии – свои или друзей.

Правильное ведение дневника может дать детям и их родителям возможность общаться и поделиться друг с другом опытом; дети могут поведать родителям о новых технологиях, а родители могут дать ряд ценных жизненных советов.

Другое преимущество – привитие ответственности и дисциплины ведения дневника; возможность творческого самовыражения; новые возможности общения с друзьями и родственниками, обучение компьютерным и Интернет-технологиям, а также развитие навыков набора на клавиатуре, правописания, письменной речи и редактирования.

ОСНОВЫ БЕЗОПАСНОГО ВЕДЕНИЯ ИНТЕРНЕТ-ДНЕВНИКА.

Требуйте от ваших детей никогда не публиковать в них какую-либо личную информацию, в том числе фамилию, контактную информацию, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения.

Требуйте от ваших детей никогда не помещать в журнале провокационные фотографии, свои или чьи-либо еще, и всегда проверять, не раскрывают ли изображения или даже задний план фотографий какую-либо личную информацию.

Пусть ваши дети знают, что публикуемая в Интернете информация остается там надолго и кто угодно может легко распечатать веб-журнал или сохранить его на своем компьютере.

Рекомендуйте детям пользоваться веб-журналами только с ясно сформулированными условиями использования и проверять, можно ли защитить с помощью пароля сами веб-журналы, а не только учетные записи пользователя (даже если это так, лучше держать в уме, что любой человек может получить доступ к Интернет-дневнику).

Рекомендуйте вашим детям не стремиться соревноваться с другими детьми, ведущими веб-журналы.

Пусть дети стараются вести свой блог в положительном ключе и не использовать его для злословия или нападок в адрес других детей.

ИГРЫ ЧЕРЕЗ ИНТЕРНЕТ: КАК ИГРАТЬ БЕЗОПАСНО

Компьютерные игры уже давно сравнялись по популярности с телевидением, музыкой и фильмами, а где-то даже превзошли их. Вы можете помочь своим детям играть в занимательные и даже поучительные игры и само собой соответствующие возрасту вашего ребенка. Нужно только придерживаться некоторых советов.

СОВЕТЫ ПО ПОВЫШЕНИЮ БЕЗОПАСНОСТИ УЧАСТИЯ ВАШИХ ДЕТЕЙ В ОНЛАЙНОВЫХ ИГРАХ ПО СЕТИ.
Получите информацию. Ознакомьтесь с классификацией игр и условиями конфиденциальности, а также прочтите правила на сайте игры. В качестве примера можно познакомиться с кодексом поведения Xbox® Live.

Будьте в курсе, в какие игры и с кем играют ваши дети. Поместите компьютер или игровую консоль (например, Xbox) туда, где экран хорошо просматривается; искренне интересуйтесь, во что дети играют.

Установите правила. Это следует сделать до выхода детей в Интернет; кроме того, убедитесь, что ребенок их понимает. С примером такого рода домашних правил можно ознакомиться, прочитав «Внутрисемейные правила пользования Интернетом» (см. с. 34 данного издания).

Контролируйте чат и сообщения во время игр. Попросите детей сообщать вам, если другой игрок употребляет нецензурные слова; в этом случае можно выделить обидчика в списке и отключить или заблокировать его сообщения. Другой вариант – сообщить о некорректно ведущем себя игроке администраторам игры по электронной почте, в чате или другим способом. Для дополнительной информации о возможных мерах воздействия на таких игроков можно обратиться на официальный сайт игры.

Обучите детей навыкам безопасности. Скажите детям, что, если кто-либо из игроков будет вести себя оскорбительно, игру следует остановить и немедленно сообщить вам. При необходимости – связаться с администратором.

Убедитесь в конфиденциальности. Требуйте от детей никогда не выдавать в игровом чате личную информацию (например, имя, пол или домашний адрес), фотографии и не соглашаться на встречи. Убедитесь, что дети знают о необходимости обратиться к вам за помощью в случае чего.
Выбирайте соответствующие имена. Заставьте ребенка использовать подходящие имена героев, соответствующие игровым правилам. Эти имена не должны раскрывать никакую личную информацию или провоцировать домогательство.

Примечание: Для компьютеров и игровых консолей типа Xbox есть технология маскировки или скрытия голоса, позволяющая изменить настоящий голос ребенка. Имейте в виду, что взрослые также могут пользоваться этой программой и выдавать себя не за того, кто они есть на самом деле.

Берегитесь хулиганов. См. с. 17 данного издания о том, как поступать с задирами (гриферами) в Интернет-играх.

Играйте вместе. Безопаснее всего для детей играть через Интернет вместе с вами. Возможно, им этого хочется меньше всего на свете (особенно тем, кто постарше), но это очень хороший способ научиться общению в Сети.

ИНТЕРНЕТ-ХУЛИГАНСТВО: КАК ПРИ ЭТОМ СЕБЯ ПРАВИЛЬНО ВЕСТИ?

Так же как и в обычной жизни, в Интернете появились свои хулиганы, которые осложняют жизнь другим пользователям Интернета.

КТО ТАКИЕ ИНТЕРНЕТ-ХУЛИГАНЫ И ЧТО ОНИ ДЕЛАЮТ? Их называют гриферами, задирами, дурными игроками, повернутыми и т.д. Есть вероятность, что один из таких злодеев по крайней мере единожды побеспокоит вашего ребенка в таких многопользовательских играх, как Halo 2, EverQuest, The Sims Online, SOCOM и Star Wars Galaxies. Обидчики (гриферы), по сути, те же дворовые хулиганы; они получают удовольствие, хамя и грубя окружающим.

Обычно хулиганы издеваются над другими, особенно над начинающими (чайниками); мешают играть товарищам по команде; используют нецензурную лексику; жульничают; создают вместе с другими гриферами бродячие банды; блокируют выходы из комнат; выманивают монстров на неосторожных игроков или используют игру, чтобы досаждать, кому только можно, или изводить конкретного человека. Хотя они составляют лишь малую часть от общего числа пользователей, из-за гриферов некоторые компании потеряли клиентов. В итоге многие разработчики игр не жалеют этих хулиганов и используют любые методы для их вычисления.

КАК ПОСТУПАТЬ, ЕСЛИ ДЕТИ СТОЛКНУЛИСЬ С ГРИФЕРАМИ? Пусть ваши дети их игнорируют. Если ребенок не будет реагировать на их воздействия, большинству гриферов это, в конце концов, надоест и они уйдут.

Посоветуйте детям изменить параметры игры. Добейтесь, чтобы ребенок играл в игры, правила или режимы которых можно изменить, например, невозможность убить товарищей по команде. Таким образом, тактика гриферов становится бессмысленной.

Порекомендуйте создать частную игру. Большинство многопользовательских игр позволяет создавать закрытые комнаты, куда можно пускать только друзей.

Пусть дети играют на сайтах со строгими правилами. Там, где установлены строгие правила, администратор сможет немедленно заблокировать хулиганов.

Пусть играют в игры, где от гриферов можно легко избавиться. Предложите ребенку играть в те игры, где сообщения хулиганов можно отключить или проголосовать за их исключение из игры.

Придумайте еще что-нибудь. Если обидчик продолжает беспокоить вашего ребенка, добейтесь, чтобы он сменил игру или сделал перерыв и вернулся позже.

Сообщайте о «дырах» в игре. Поищите вместе с ребенком уязвимости в игре или новые способы жульничества. Сообщайте о своих находках администратору.

Пусть ваши дети воздерживаются отвечать огнем на огонь. Убедитесь, что ребенок не использует против обидчиков их же тактику; скорее всего, это спровоцирует гриферов на еще более озлобленное поведение. Или, что еще хуже, создаст о ребенке впечатление как об обидчике.

Рекомендуйте детям избегать провокаций с именами. Ребенок избежит многих проблем, если не станет использовать псевдоним, который может спровоцировать обидчика.

Пусть дети не выдают личную информацию. Хулиганы (да и вообще кто угодно) могут использовать настоящие имена, номера телефонов, а также домашние или электронные адреса, чтобы причинить ребенку неприятности.

КАК УБЕРЕЧЬСЯ ОТ НЕДОСТОВЕРНОЙ ИНФОРМАЦИИ?

Интернет предлагает колоссальное количество возможностей для обучения, но есть и большая доля информации, которую никак нельзя назвать ни полезной, ни надежной. Пользователи Сети должны мыслить критически, чтобы оценить точность материалов; поскольку абсолютно любой может опубликовать информацию в Интернете.

Это, в частности, относится к детям, которые склонны думать: «Раз в Интернете – значит, правильно. У газет или журналов есть проверяющие люди: корректор и редактор. Но Интернет не сможет проверить, насколько правдива размещенная информация.

Расскажите детям, как работает Интернет, и объясните, что каждый может создать сайт и никто ему не задаст никаких вопросов. Научите детей использовать широкий круг источников и проверять все, что они видят в Сети.

КАК НАУЧИТЬ ДЕТЕЙ ОПРЕДЕЛЯТЬ ЛОЖНЫЕ МАТЕРИАЛЫ? Начинайте, когда дети еще маленькие. Теперь, когда даже дошкольники используют Интернет, важно научить их отличать факты от мнений как можно раньше.

Спрашивайте детей о найденной ими в Интернете информации. Например, для чего нужен этот сайт? Для развлечений? Продажи товара? Есть ли на сайте контактная информация или раздел «О нас»? Спонсируется ли сайт кем-то или это место общественной дискуссии? И подумайте: является ли Интернет наилучшим местом для поиска именно этой информации?

Убедитесь, что дети проверяют собранную в Сети информацию по другим источникам. Для проверки материалов обратитесь к другим сайтам или СМИ – газетам, журналам и книгам. Приучите детей советоваться с вами.

Поощряйте использование детьми разных источников. Возьмите их с собой в библиотеку или приобретите для них энциклопедию на диске. Это даст детям доступ к альтернативным источникам информации. Научите детей эффективным способам поиска. Это сильно увеличит их возможности получения качественной информации. Один из способов – приучить детей пользоваться не одной поисковой машиной, а несколькими.

МАТЕРИАЛЫ НЕЖЕЛАТЕЛЬНОГО СОДЕРЖАНИЯ: КАК ИЗБЕЖАТЬ?

ЧТО ЗНАЧИТ НЕЖЕЛАТЕЛЬНОЕ СОДЕРЖАНИЕ. Как правило, большинство родителей не склонны поощрять знакомство своих детей с материалами порнографического, ненавистнического содержания, материалами суицидальной направленности, сектантскими материалами, ненормативной лексикой. Такую информацию относят к материалам нежелательного характера.

Если порнографические материалы или материалы с ненормативной лексикой можно относительно легко идентифицировать и отсечь с помощью средств фильтрации, то от нежелательных материалов других типов детей защитить гораздо сложнее.

Например, на детских сайтах могут встречаться самые разные формы выражения ненависти: от радикального расизма до грубого высмеивания. Такие сайты на первый взгляд могут казаться безобидными, но они вносят свой вклад в формирование детской онлайновой культуры, в которой грубость по отношению к другим считается допустимой.

Расисты и группы ненависти стали использовать Интернет для привлечения молодежи в свои ряды. Последние ищут восприимчивых молодых людей, а

затем вовлекают их в свое сообщество, используя для этого чаты и электронную почту.

Некоторые ненавистнические сайты создают разделы специально для детей. Эта часть сервера специально имеет располагающий вид, предлагает безобидные игровые занятия и дает ссылки на уважаемые сайты.

КАК ПОМОЧЬ СВОИМ ДЕТЯМ ИЗБЕЖАТЬ НЕНАВИСТНИЧЕСКИХ МАТЕРИАЛОВ?

Используйте средства фильтрации нежелательного материала (например, MSN Premium's Parental Controls или встроенные в Internet Explorer®) . Но фильтры могут только помочь в блокировании некоторых нежелательных материалов, они не могут полностью решить проблему. Выражения ненависти, встречающиеся в Интернете, часто принимают мягкие формы и не всегда распознаются фильтрами. Поэтому важно поддерживать доверительные отношения с детьми, чтобы они без колебаний обращались к вам за помощью.

Контролируйте использование Интернета и наблюдайте за детьми. Как правило, дети, не достигшие десятилетнего возраста, еще не имеют навыков критического мышления, необходимого для самостоятельного посещения Сети.

Расскажите детям о существующих в Интернете способах выражения ненависти. Научите их распознавать материалы с ненавистническим содержанием и символикой, например, изображение свастики, оскорбительные отзывы о расовой принадлежности, карикатурные описания разных этнических и расовых групп. Вашим детям будет легче избежать материалов ненавистнического содержания, если они будут знать об истории расизма, шовинизма и стратегиях распространителей ненависти.

Младшим детям нужно подробно объяснить, что это за материалы, для чего их публикуют, какие опасности они несут, в чем состоит вред расовых концепций.

Старших детей необходимо научить критически относиться к содержанию онлайновых материалов и не доверять им без совета с вами.