Родительский контроль и безопасный интернет

Тема посвященная информационной безопасности детей и действиям родителей по предотвращению доступа детей к информации в сети интернет, на электронных носителях, в играх, по телевидению, которая может навредить их психическому развитию, несет угрозу безопасности ребенка.

Мы и не думали никогда, что воспитание ребенка будет сопряжено с опасностями, таящимися в интернете. Раньше было просто: получил двойку – отец хмур, как грозовые тучи, ударил девочку во дворе – мать читает нотации о высоких нравах. Жизненных ситуаций, где ребенок способен нашкодить, множество, но тут, откуда не возьмись, добавилась еще одна проблема – детишки полезли в интернет. А там их ждет множество опасностей, о которых они сами, скорее всего, даже и не подозревают.

Как бы банально это не звучало, но все решает воспитание. Ребенку надо показать интернет, заинтересовать полезными, с вашей точки зрения, сайтами, объяснить, что можно делать, а что нельзя. Нельзя соглашаться на встречи с незнакомыми людьми, нельзя сообщать личные данные, нельзя самостоятельно совершать покупки в сетевых магазинах. Ну а вместо нравоучений сыну «не смотри на голых женщин», уместней воспользоваться специальными программными продуктами, которые закроют ему доступ к взрослым ресурсам.

Несколько советов разработанных интернет специалистами Фонда развития интернета и Центра безопасного интернета в России

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.

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.

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 также неприятно, как и слышать;

- Научите детей правильно реагировать на обидные слова или действия других

пользователей;

- 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.

Даже при самых доверительных отношениях в семье родители иногда не могут вовремя заметить грозящую ребенку опасность и, тем более, не всегда знают, как ее предотвратить.

Вот на что следует обращать внимание родителям, чтобы вовремя заметить, что ребенок стал жертвой кибербуллинга:

- Беспокойное поведение

- Даже самый замкнутый школьник будет переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и нежелание идти в школу – самые явные признаки того, что ребенок подвергается агрессии.

- Неприязнь к Интернету.

- Если ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В очень редких случаях детям действительно надоедает проводить время в Сети. Однако в большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире.

- Нервозность при получении новых сообщений.

- Негативная реакция ребенка на звук письма на электронную почту должна насторожить родителя. Если ребенок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.

Как научить ребенка быть осторожным в Сети и не стать жертвой интернет-мошенников

Кибермошенничество — один из видов киберпреступления, целью которого является обман пользователей: незаконное получение доступа либо хищение личной информации (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный или иной ущерб.

Предупреждение кибермошенничества:

- Проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете;

- Установите на свои компьютеры антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных системах, наиболее частым из которых является кража конфиденциальных данных.

Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности и, если Ваш ребенок уже совершает онлайн-покупки самостоятельно, объясните ему простые правила безопасности:

- Ознакомьтесь с отзывами покупателей

- Проверьте реквизиты и название юридического лица – владельца магазина

- Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис WhoIs)

- Поинтересуйтесь, выдает ли магазин кассовый чек

- Сравните цены в разных интернет-магазинах

- Позвоните в справочную магазина

- Обратите внимание на правила интернет-магазина

- Выясните, сколько точно вам придется заплатить

Как распознать интернет- и игровую зависимость

Сегодня все более актуальны проблемы так называемой «интернет-зависимости» (синонимы: интернет-аддикция, виртуальная аддикция) и зависимости от компьютерных игр («геймерство»). Первыми с ними столкнулись врачи-психотерапевты, а также компании, использующие в своей деятельности Интернет и несущие убытки, в случае, если у сотрудников появляется патологическое влечение к пребыванию онлайн.

Согласно исследованиям Кимберли Янг, предвестниками интернет-зависимости являются:

- навязчивое стремление постоянно проверять электронную почту;

- предвкушение следующего сеанса онлайн;

- увеличение времени, проводимого онлайн;

- увеличение количества денег, расходуемых онлайн.

Если Вы считаете, что Ваши близкие, в том числе дети, страдают от чрезмерной увлеченности компьютером, это наносит вред их здоровью, учебе, отношениям в обществе, приводит к сильным конфликтам в семье, то Вы можете обратиться к специалистам, занимающимся этой проблемой. Они помогут построить диалог и убедить зависимого признать существование проблемы и согласиться получить помощь. Помощь может быть оказана как в специальных терапевтических группах, так и стационарно, с использованием специальных медицинских процедур.

Как научить ребенка не загружать на компьютер вредоносные программы

Вредоносные программы (вирусы, черви, «троянские кони», шпионские программы, боты и др.) могут нанести вред компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными и даже использовать Ваш компьютер для распространения вируса, рассылать от Вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Предупреждение столкновения с вредоносными программами:

- Установите на все домашние компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери данных. Такие приложения наблюдают за трафиком и могут предотвратить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.

Предупреждение столкновения с вредоносными программами:

- Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр.

- Объясните ребенку, как важно использовать только проверенные информационные ресурсы и не скачивать нелицензионный контент.

- Периодически старайтесь полностью проверять свои домашние компьютеры.

- Делайте резервную копию важных данных.

- Старайтесь периодически менять пароли (например, от электронной почты) и не используйте слишком простые пароли.

Что делать, если ребенок все же столкнулся с какими-либо рисками в сети

- Установите положительный эмоциональный контакт с ребенком, расположите его к разговору о том, что случилось. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен Вам доверять и знать, что Вы хотите разобраться в ситуации и помочь ему, а не наказать;

- Постарайтесь внимательно выслушать рассказ о том, что произошло, понять насколько серьезно произошедшее и насколько серьезно это могло повлиять на ребенка;

- Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети), или он попал в неприятную ситуацию (потратил Ваши или свои деньги в результате интернет-мошенничества и пр.) — постарайтесь его успокоить и вместе с ним разберитесь в ситуации — что привело к данному результату, какие неверные действия совершил сам ребенок, а где Вы не рассказали ему о правилах безопасности в Интернете;

- Если ситуация связана с насилием в Интернете по отношению к ребенку, то

необходимо выяснить информацию об агрессоре, выяснить историю взаимоотношений ребенка и агрессора, выяснить существует ли договоренность о встрече в реальной жизни; узнать были ли такие встречи и что известно агрессору о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т.п.), жестко настаивайте на избегании встреч с незнакомцами, особенно без свидетелей, проверьте все новые контакты ребенка за последнее время;

- Соберите наиболее полную информацию о происшествии, как со слов ребенка, так и с помощью технических средств — зайдите на страницы сайта, где был Ваш ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию — в дальнейшем это может Вам пригодиться (например, для обращения в правоохранительные органы);

- Если Вы не уверены в оценке серьезности произошедшего с Вашим ребенком, или ребенок недостаточно откровенен с Вами или вообще не готов идти на контакт, или Вы не знаете как поступить в той или иной ситуации — обратитесь к специалисту (телефон доверия, горячая линия и др.), где Вам дадут рекомендации о том, куда и в какой форме обратиться, если требуется вмешательство других служб и организаций (МВД, МЧС, Сестры и др.)

Программы родительского контроля предназначены, в первую очередь, для создания ограничений ребенку, они призваны обеспечить его безопасность, оградить от того, что, возможно, ему еще рано знать и видеть. Одна из основных задач приложений – создание фильтра web-сайтов. Все очень просто: на одни страницы заходить можно, на другие – нельзя. Как осуществляется подобный контроль? Обычно предлагается два варианта ограничений.

Приложение работает с базой данных, где содержатся сайты для взрослых. Крайне желательно, чтобы список регулярно обновлялся через интернет, иначе появление новых ресурсов быстро сделает защиту неактуальной. Администратор или, в данном случае, родители могут расширять черный список сайтов на свое усмотрение.

В вашей семье один ребенок или несколько детей, есть компьютер, подключенный к интернету. Как обезопасить младшее поколение от негативных последствий пребывания в Сети? Первое, что сразу напрашивается – компьютер не должен стоять в детской комнате. Лучше всего, если он будет в зале, где кто-нибудь из родителей сможет постоянно следить за тем, чем занимается ребенок. В противном случае, он запрется в комнате, и вы даже, возможно, не догадаетесь, что чадом скачано несколько фильмов эротического содержания, а в местном чате ему рассказали, как самому делать петарды.

ПРОГРАММЫ РОДИТЕЛЬСКОГО КОНТРОЛЯ

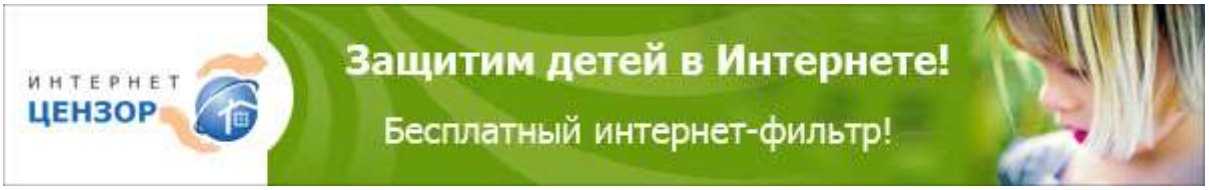
Crawler Parental Control 1.1, KidsControl 2.02, ParentalControl Bar 5.22, Spector Pro 6.0, КиберМама и множество других

ЕСЛИ ВЫ ИСПОЛЬЗУЕТЕ НА ДОМАШНЕМ КОМПЬЮТЕРЕ ОПЕРАЦИОННУЮ СИСТЕМУ **WINDOWS**, ТО НАЧИНАЯ С ВЕРСИИ - **VISTA И ВЫШЕ**, ВЫ МОЖЕТЕ ЗАДЕЙСТВОВАТЬ **ВСТРОЕННЫЕ СРЕДСТВА РОДИТЕЛЬСКОГО КОНТРОЛЯ** В НАСТРОЙКАХ СИСТЕМЫ.

Интернет Цензор - интернет-фильтр, предназначенный для блокировки потенциально опасных для здоровья и психики подростка сайтов.

В основе работы программы лежит технология "белых списков", гарантирующая 100% защиту от опасных и нежелательных материалов. Программа содержит уникальные вручную проверенные "белые списки", включающие все безопасные сайты Рунета и основные иностранные ресурсы. Программа надежно защищена от взлома и обхода фильтрации.

Интернет Цензор может использоваться как в домашних условиях, так и в организациях – образовательных учреждениях, библиотеках, музеях, интернет-кафе и иных местах, где возможно предоставление несовершеннолетним доступа в Интернет.



Родительский контроль и безопасный интернет

ФЕДЕРАЛЬНАЯ ПРОГРАММА БЕЗОПАСНОГО ДЕТСКОГО ИНТЕРНЕТА «ГОГУЛЬ»

Детский интернет-браузер Гогуль - это программа для ограничения доступа в интернет и фильтрации содержимого веб-ресурсов, для обеспечения безопасности ребёнка и родительского контроля детского сёрфинга по сети.

Безопасность ребёнка в интернете обеспечивается за счёт каталога детских сайтов, проверенных педагогами и психологами, и насчитывающего тысячи детских интернет-сайтов.

Гогуль ведёт статистику посещённых сайтов для родительского контроля интернет-сёрфинга ребёнка, а также может ограничивать время пребывания детей в интернете.

Скачать Детский интернет-браузер Гогуль