**РЕКОМЕНДАЦИИ ДЛЯ РОДИТЕЛЕЙ**

Интернет является прекрасным источником для новых знаний, помогает в учебе, занимает досуг. Но в, то, же время, Сеть таит в себе много опасностей. Обязательно нужно поговорить с детьми, объяснить, что могут возникать различные неприятные ситуации и то, как из них лучшим образом выходить. Помните, что безопасность ваших детей в Интернете, на 90% зависит от вас.

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 обратить 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:

1.  Проинформировать ребенка о самых распространенных методах мошенничества и научить его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете;

2.  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;

3.  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 в России все более актуальны проблемы так называемой «интернет-зависимости» 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 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.

−    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**

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.)

**Как защитить детей от негативной информации?**

В связи с развитием новых технологий в области виртуального пространства, в том числе с распространением сети Интернет, возникла проблема, связанная с доступом несовершеннолетних к информации сомнительного содержания и противоречащей общепринятой этике. В настоящее время любой человек, в том числе и несовершеннолетний, владеющий знаниями в области компьютерных технологий, может получить доступ к данным, хранящимся в Интернете, или создать свой собственный веб - ресурс. Отсутствие контроля со стороны родителей за использованием детьми сети Интернет - одна из причин доступности негативной информации несовершеннолетним. Памятка родителям по безопасному использованию детьми сети Интернет. Основные правила, которые помогут оградить Ваших детей от информации сомнительного содержания и противоречащей общепринятой этике.

Правило №1   Родители должны знать интересы и цели детей, которые используют сеть Интернет.

Правило №2  Рекомендуется допускать использование сети Интернет детьми в присутствии взрослых. Доступ к данному информационному ресурсу должен быть эффективным и безопасным.

Правило №3 Необходимо исключить доступ детей к ресурсам сети Интернет, содержание которых противоречит законодательству Российской Федерации, может оказать негативное влияние на несовершеннолетних (информацию, пропагандирующую порнографию, культ насилия и жестокости, наркоманию, токсикоманию, антиобщественное поведение, сайты, содержащие описание или изображение убийств, мертвых тел, насилия и т.п.).

Правило №4    В случае самостоятельного доступа детей к сети Интернет, родители должны контролировать использование информации несовершеннолетними. О характере и объеме информации, полученной детьми в интернет – ресурсах, необходимо узнавать в «Журнале обозревателя» программы "Internet Explorer" . Как ограничить доступ детей к негативной информации в сети Интернет? С целью ограничения доступа детей к «вредным» материалам родители и другие члены семьи могут установить на компьютеры программу «Касперский Интернет секьюрити 2010»: в настройке программы применить вкладку «Родительский контроль», при этом произойдет блокировка информации, связанной с порнографическими сюжетами, жестокостью, нецензурной лексикой и др., оказывающей негативное влияние на детей и подростков.

**Семейное соглашение о работе в Интернет**

Если ваши дети хотят посещать Интернет, вам следует выработать вместе с ними соглашение по использованию Интернет. Учтите, что в нем вы должны однозначно описать права и обязанности каждого члена вашей семьи. Не забудьте четко сформулировать ответы на следующие вопросы:

−        Какие сайты могут посещать ваши дети и что они могут там делать;

−        Сколько времени дети могут проводить в Интернет;

−        Что делать, если ваших детей что-то беспокоит при посещении Интернет;

−        Как защитить личные данные;

−        Как следить за безопасностью;

−        Как вести себя вежливо;

−        Как пользоваться чатами, группами новостей и службами мгновенных сообщений.

Не забудьте, что формально составленное соглашение не будет выполняться! Регулярно, по мере необходимости, вносите изменения в данное соглашение. Не забывайте, что вы должны проверять выполнение соглашения вашими детьми.

**Может ли ваш ребенок стать интернет-зависимым?**

Не забывайте, что Интернет это замечательное средство общения, особенно для стеснительных, испытывающих сложности в общении детей. Ведь ни возраст, ни внешность, ни физические данные здесь не имеют ни малейшего значения. Однако этот путь ведет к формированию Интернет-зависимости. Осознать данную проблему весьма сложно до тех пор, пока она не становится очень серьезной. Да и кроме того, факт наличия такой болезни как Интернет-зависимость не всегда признается. Что же делать?

Установите правила использования домашнего компьютера и постарайтесь найти разумный баланс между нахождением в Интернет и физической нагрузкой вашего ребенка. Кроме того, добейтесь того, чтобы компьютер стоял не в детской комнате, а в комнате взрослых. В конце-концов, посмотрите на себя, не слишком ли много времени вы проводите в Интернет.

**Возраст от 7 до 8 лет**

Как считают психологи, для детей этого возраста абсолютно естественно желание выяснить, что они могут себе позволить делать без разрешения родителей. В результате, находясь в Интернет ребенок будет пытаться посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей.

Поэтому в данном возрасте особенно полезны будут те отчеты, которые вам предоставит Родительский контроль или то, что вы сможете увидеть во временных файлах Интернет (папки c:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files в операционной системе).

В результате, у вашего ребенка не будет ощущения, что вы глядите ему через плечо на экран, однако, вы будете по-прежнему знать, какие сайты посещает ваш ребенок.

Стоит понимать, что дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Дети этого возраста любят играть в сетевые игры и путешествовать по Интернет. Вполне возможно, что они используют электронную почту и могут заходить на сайты и чаты, не рекомендованные родителями.

По поводу использования электронной почты хотелось бы заметить, что в данном возрасте рекомендуется не разрешать иметь свой собственный электронный почтовый ящик, а пользоваться семейным, чтобы родители могли контролировать переписку.

Помочь вам запретить ребенку использовать внешние бесплатные ящики сможет такое программное обеспечение, как Kaspersky Internet Security версии 7.0 со встроенным родительским контролем.

**Что можно посоветовать в плане безопасности в таком возрасте?**

−    Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения;

−    Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером;

−    Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь;

−   Приучите детей, что они должны посещать только те сайты, которые вы разрешили, т.е. создайте им так называемый «белый» список Интернет с помощью средств  Родительского контроля. Как это сделать, мы поговорим позднее;

−    Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей;

−    Используйте специальные детские поисковые машины, типа MSN Kids Search;

−    Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю;

−    Создайте семейный электронный ящик чтобы не позволить детям иметь собственные адреса;

−    Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО;

−  Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей;

−    Научите детей не загружать файлы, программы или музыку без вашего согласия;

−   Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или содержащих определенные слова или фразы.

−    Не разрешайте детям использовать службы мгновенного обмена сообщениями;

−    В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией;

−    Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни;

−   Не делайте «табу» из вопросов половой жизни, так как в Интернет дети могут легко наткнуться на порнографию или сайты «для взрослых»;

−  Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

−     Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами;

−     Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

  Базовые правила безопасного Интернета для детей

**НЕЛЬЗЯ**

−    Всем подряд сообщать свою частную информацию (настоящие имя, фамилию, телефон, адрес, номер школы, а также фотографии свои, своей семьи и друзей)

−    Нельзя открывать вложенные файлы электронной почты, когда не знаешь отправителя

−    Нельзя рассылать самому спам и «информационную грязь»

−    Нельзя грубить, придираться, оказывать давление — вести себя невежливо и агрессивно

−    Никогда не распоряжайся деньгами твоей семьи без разрешения старших. Спроси родителей.

−    Встреча с Интернет-знакомыми в реальной жизни, бывает опасной: за псевдонимом может скрываться преступник

**ОСТОРОЖНО**

−    Не все пишут правду

−    Читаешь о себе неправду в Интернете — сообщи об этом своим родителям или опекунам

−    Приглашают переписываться, играть, обмениваться – проверь, нет ли подвоха

−    Незаконное копирование файлов в Интернете = воровство

−    Открыл что-то угрожающее — не бойся позвать на помощь

**МОЖНО**

−    Используй «ник» (выдуманное имя) в переписке и переговорах

−    Уважай другого пользователя

−    Пользуешься Интернет-источником – делай ссылку на него

−    Познакомился в сети и хочешь встретиться – посоветуйся со взрослым, которому доверяешь

−    Открывай только те ссылки, в которых уверен

−   Интернетом лучше всего пользоваться, когда поблизости есть кто-то из родителей или тех, кто хорошо знает, что такое Интернет, и как в нем себя вести.

* Составьте список правил работы детей в Интернете и помните, что лучше твердое «нет», чем неуверенное «да». Пусть ограничения будут минимальны, но зато действовать всегда и без ограничений.
* Расскажите детям о **необходимости сохранения конфиденциальных данных в тайне**и о том, как лучше это сделать. Вот несколько простых правил, которых следует придерживаться:  
  - при общении использовать только имя или псевдоним (ник);  
  - номер телефона, свой адрес, место учебы **нельзя никому сообщать**;  
  - не пересылать свои фотографии;  
  - без контроля взрослых не встречаться с людьми, знакомство с которыми завязалось в Сети.
* Поясните, что в сети, несмотря на кажущуюся безнаказанность за какие-то проступки, там действуют те же правила, что и в реальной жизни: хорошо - плохо, правильно - не правильно.
* Научите детей развивать и доверять интуиции. **При малейших признаках беспокойства, путь рассказывают об этом вам**.
* Если детям по каким-либо причинам нужно вводить регистрационное имя, помогите его придумать так, чтобы оно не несло в себе никакой личной информации.
* Объясните, что люди в Сети часто выдают себя совсем за других. Поэтому встречаться с ними не стоит.
* Научите детей следовать нормам морали, быть воспитанными даже в виртуальном общении.
* Обязательно расскажите о правах собственности, о том, что любой материал, выставленный в Сети, может быть авторским. Неправомерное использование такого материала может быть уголовно наказуемым.
* объясните, что **далеко не все, что можно увидеть в Интернете – правда**. При сомнениях, пусть лучше уточнит у вас.
* Используйте современные программы, которые предоставляют возможность фильтрации содержимого сайтов, контролировать места посещения и деятельность там.
* Создайте доверительные отношения между вами и вашим ребенком. **Посещайте его любимые сайты**иногда вместе, если ребенок ведет дневник, время от времени прочитывайте его.
* Внимательно относитесь к вашим детям!