**Совет по Интернет – безопасности**

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:

1. Проверьте реквизиты и название юридического лица – владельца магазина

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

3. Поинтересуйтесь, выдает ли магазин кассовый чек

4. Сравните цены в разных интернет-магазинах.

5. Позвоните в справочную магазина

6. Обратите внимание на правила интернет-магазина

7. Выясните, сколько точно вам придется заплатить

**Как распознать интернет- и игровую зависимость**

Сегодня в России 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.
* 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.

**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