Правила безопасности в Интернете

Реальность, в которой живут современные дети и подростки, несравнима с той, в которой воспитывались их родители.

Использование разнообразных информационных ресурсов оказывает значительное положительное воздействие на развитие детей – это увлекательно, это обучает и социализирует. Но не все понимают, что эти же средства могут представлять потенциальную угрозу в зависимости от того, как осуществляется их использование.

С какими угрозами могут столкнуться дети в сети Интернет?

1. Коммуникационные риски или риски общения

✔ *Интернет-хулиганство, киберпреследование, киберзапугивание (кибербуллинг).*Кибербуллинг – психологическое насилие в сети, информационное преследование со стороны сверстников, проявляющееся в виде издевательств, насмешек, запугиваний, прочих действий, которые негативно влияют на психическое состояние ребенка. У него создается ощущение безысходности, даже дома его не оставляет чувство тревоги, он впадает в депрессию. Информационная атака может привести к суициду.

Издевательство в сети наказуемо действующим законодательством. Согласно статьям 152, 153 Гражданского кодекса Республики Беларусь человек, которого оскорбили, может обратиться в суд с исковым заявлением о защите чести и достоинства. Также оскорбившего можно привлечь к административной ответственности по статье 10.2 Кодекса Республики Беларусь об административных правонарушениях. Для этого необходимо обратиться в отдел внутренних дел по месту жительства с заявлением.

✔ *Знакомства в Интернете и встречи с Интернет-незнакомцами.*

Общаясь в сети, дети могут знакомиться, общаться и добавлять в «друзья» совершенно неизвестных им в реальной жизни людей.

Социологические опросы об информационной безопасности детей и подростков в Интернет-сети приводят следующие данные о контактах: родственники – 43 %; виртуальные друзья – 21%; незнакомые люди – 36%. Однако по большому счету виртуальные друзья – тоже незнакомцы. Таким образом, большую часть своего времени в сети дети уделяют общению с посторонними людьми, делятся своими переживаниями, секретами, планами. В таких ситуациях есть опасность разглашения ребенком личной информации о себе и своей семье. Каждое слово, каждая выложенная фотография, каждое действие в сети могут быть использованы против ребенка, и представляет собой благодатную почву для шантажа в будущем.

Особенно опасным может стать установление дружеских отношений с ребенком с целью личной встречи (груминг), вступления с ним в сексуальные отношения, шантажа и эксплуатации. Обман детей возможен, так как при общении в интернете не всегда точно можно сказать, кто на самом деле является твоим собеседником. Часто этим приемом пользуются педофилы, которые общаются с детьми от лица другого «ребенка» и предлагают встретиться в реальной жизни.

2. Потребительские риски

Сюда относится хищение персональной информации с целью кибермошенничества. Хищение конфиденциальных данных может привести к тому, что мошенник незаконно получает доступ и каким-либо образом использует личную информацию пользователя с целью получить материальную прибыль.

По информации пресс-службы Министерства внутренних дел Республики Беларусь зафиксируется 25,5 тысяч преступлений в сфере высоких технологий. Из них 23,5 тысячи – хищение денег с использованием компьютерной техники. Очень часто злоумышленники звонят в мессенджерах (приложения для переписки) якобы из банка и под разными предлогами узнают реквизиты, пин-код, трехзначный код на оборотной стороне карты.

Сваттинг – это новый для Беларуси вид преступления. Хулиганы-геймеры отправляют в экстренные службы ложное сообщение об опасности от имени другого игрока. Во-первых, ложные сообщения отвлекают от оказания помощи тем, кто в ней действительно нуждается. Во-вторых, такими «разводами» геймеры могут доставить большие неприятности с законом своим оппонентам. По всему миру милиция успешно устанавливает личности этих геймеров.

В Беларуси за «сваттинг» предусмотрена ответственность по статье 340 Уголовного кодекса Республики Беларусь до 7 лет лишения свободы. Если геймер не достиг возраста привлечения к уголовной ответственности, то отвечать за него придется родителям.

Мошенники и способы их действия идут в ногу со временем. Неосведомленность и наивность детей делают их легкой добычей. Один из способов обмана – это «выигрыш». Сообщение о призе (компьютер, мобильный телефон и пр.). Для этого у несовершеннолетних просят сообщить данные электронной карты (родителей) и цифры, которые пришли в СМС-сообщении на телефонный номер.

Также среди киберпреступлений распространен фишинг – когда в социальную сеть сбрасывают вредоносную ссылку, по которойчеловек попадает на поддельный сайт и «засвечивает» все данные своей платежной карты, после чего приходит сообщение о списании денег.

Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации – наказывается штрафом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок (ст. 212 Уголовного кодекса Республики Беларусь). За совершенные преступления ребенком в возрасте до 14 лет несут ответственность их родители.

Рекомендации для родителей по безопасности детей в сети интернет

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.

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 по телефону доверия 170. Кроме того, ответы на вопросы, связанные с проблемой кибербуллинга, а также анонимную консультацию психолога можно получить на сайте http://kids.pomogut.by, созданном по инициативе Министерства внутренних дел Республики Беларусь, а также на детском правовом сайте https://mir.pravo.by.

Памятка родителям по безопасности ребенка в сети интернет

Первое. Расскажите ребенку, что представляет собой Интернет-пространство, чем полезен Интернет, что можно там найти интересного и что негативного можно встретить. Лучше представить виртуальную сеть как помощника в поиске информации или как средство образования, а не как возможность для развлечений и удовольствий, чтобы ребенок не просиживал все свободное время в сети, а правильно распределял его по необходимости.

Второе. Договоритесь с ребенком, сколько времени он будет проводить в сети. Для каждого возраста должно быть свое время – чем старше ребенок, тем больше он может находиться в сети, но определенные рамки все равно должны сохраняться. Десятилетнему ребенку достаточно и 30 минут. Можно создать список домашних правил пользования Интернетом, где будет указан перечень сайтов, которые можно посещать, информация о защите личных данных, этика поведения в сети и прочее.

Третье. Предупредите свое чадо о том, что в сети он может столкнуться с запрещенной информацией и злоумышленниками. Речь идет о насилии, наркотиках, порнографии, страницах с националистической или откровенно фашистской идеологией. Ведь все это доступно в Интернете без ограничений. Часто случается так, что просмотр подобной информации даже не зависит от ребенка – на многих сайтах отображаются всплывающие окна, содержащие любую информацию, чаще всего порнографического характера. При столкновении с негативным контентом ребенок обязательно должен рассказать об этом родителям.

Четвертое. Приучите детей к конфиденциальности. Если на сайте необходимо, чтобы ребенок ввел имя, помогите ему придумать псевдоним, не раскрывающий никакой личной информации. Расскажите детям о том, что нельзя сообщать какую-либо информацию о своей семье – делиться проблемами, рассказывать о членах семьи, о материальном состоянии, сообщать адрес.

Пятое. Беседуйте с детьми об их виртуальных друзьях и о том, чем они занимаются так, как если бы речь шла о друзьях в реальной жизни. Часто педофилы регистрируются на детских сайтах, вступают в переписку с ребенком, общаются длительное время - все это для определенной цели –завоевать доверие ребенка и добиться встречи с ним. Каковы могут быть последствия встречи, догадаться несложно. Приучите детей рассказывать о встречах в реальной жизни. Если ребенок хочет встретиться с другом, он обязательно должен сообщить об этом взрослым.

Шестое. Расскажите о мошенничествах в сети - розыгрышах, лотереях, тестах, чтобы ребенок никогда, без ведома взрослых, не отправлял СМС, чтобы узнать какую-либо информацию из Интернета.

Седьмое. Объясните детям, что никогда не следует отвечать на мгновенные сообщения или письма по электронной почте, поступившие от незнакомцев. Если ребенка что-то пугает, настораживает или кто-то угрожает в переписке, в письме, он обязательно должен сообщить об этом взрослым.

Ознакомьте ваше чадо с этими простыми правилами, и он будет иметь представление о том, с чем может столкнуться в Интернете, и будет знать, как вести себя в этом случае. Если ребенок будет вам доверять и рассказывать все, что впечатлило его в сети, с кем он познакомился, вы сможете избежать очень серьезных бед, таких как похищение ребенка посредством сети и сексуальная эксплуатация детей. Но не переборщите – не надо запугивать ребенка Интернетом, говорить, что это очень опасная и страшная штука, но ей надо уметь пользоваться. Ребенок должен усвоить мысль, что Интернет – это друг, и если правильно с ним «дружить», можно извлечь из этого очень много пользы. А правильно «дружить» с ним научить может только взрослый.

Советы родителям по безопасности в сети интернет детей подросткового возраста (13-17 лет)

В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей. Тем не менее, особенно важно строго соблюдать правила интернет-безопасности – соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

В 13–17 лет подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок "для взрослых". Девочки предпочитают общаться в

чатах, при этом они гораздо боле чувствительны к сексуальным домогательствам в Интернете.

Советы по безопасности в этом возрасте.

• Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов ("черный список"), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).

• Компьютер с подключением к Интернету должен находиться в общей комнате; часы работы в Интернете могут быть легко настроены при помощи средств Родительского контроля.

• Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.

• Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

• Необходимо знать, какими чатами пользуются ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

• Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из Интернета.

• Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

• Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

• Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. 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.

• Расскажите детям о порнографии в Интернете.

• Помогите им защититься от спама. Научите подростков не выдавать в Интернет своего электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

• Приучите себя знакомиться с сайтами, которые посещают подростки.

• Объясните детям, что ни в коем случае нельзя использовать сеть для хулиганства, распространения сплетен или угроз другим людям.

• Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закона.

Как проводить Родительский контроль над поведением детей в Интернете?

Обеспечивать родительский контроль в Интернете можно с помощью различного программного обеспечения, например, Родительский контроль в WindowsVista, средства Родительского контроля, встроенные в KasperskyInternetSecurity.

Например: на компьютер можно установить программу «Касперский Интернет секьюрити 2010»; в настройке программы применить вкладку «Родительский контроль», при этом произойдет блокировка информации, связанной с порнографическими сюжетами, жестокостью, нецензурной лексикой.