Безопасность в Интернете

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 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.)

Портал о безопасности в сети Интернет

Ресурс размещен по адресу: http://www.saferunet.ru/ Портал посвящен проблеме безопасной, корректной и комфортной работы в Интернете. А конкретнее – мы занимаемся Интернет-угрозами и эффективным противодействием им в отношении пользователей. Центр был создан в 2008 году под названием "Национальный узел Интернет-безопасности в России". Центр Безопасного Интернета (Национальный Узел Интернет-безопасности в России) - член Международной сети "горячих линий" по борьбе с противоправным контентом INHOPE Центр безопасного Интернета в России - организатор мероприятий Международного Дня безопасного Интернета на территории Российской Федерации в форме Недели безопасного Рунета.

Достоверность информации в Интернете

В последние годы Интернет стал самым популярным источником информации. Это вполне закономерно, поскольку поиск данных в Сети удобен, прост и занимает гораздо меньше времени, чем поход в библиотеку, чтение архивов газет или даже просмотр телевизора. В связи с постоянным развитием Интернет-технологий, в обществе сформировалось позитивное общественное мнение о полезности Интернета, а расширение его технических возможностей и аудитории, повлекло за собой появление множества информационных сервисов и ресурсов. Поиск информации через Интернет стал прерогативой не только рядовых пользователей, но и государственных служащих, бизнесменов и коммерческих организаций. Ведь своевременное получение информации способно приносить немалую прибыль и ощутимую пользу. Коммуникация с клиентами и потребителями, доступная реклама перед потенциальной аудиторией, все это открыло массу возможностей как для потребителей, так и для распространителей информации.

Доверяй, но проверяй

Таким образом, рано или поздно перед каждым пользователем Интернета встает один неизбежный вопрос. Можно ли доверять той информации, которая публикуется в Интернете? Осуществлять контроль достоверности информации, полученной в результате поиска, не только можно, но и нужно. Доверять всему, что написано в Сети было бы слишком глупо и наивно, ведь Интернет является зоной свободного доступа, и абсолютно каждый может принимать участие в его наполнении. Рассмотрим традиционные способы проверки полученных через Интернет данных:

1. Проверка фактического материала Факт выдумать невозможно, ибо его достоверность строго установлена. Любые фактические и статистические данные имеют источник. Проверка точности фактов и приведенных чисел с большой долей вероятности покажет, на какие данные опирается сайт. Идеальным будет наличие ссылок на авторитетные источники вроде агентств сбора статистики или научные институты. Если эта информация не является точной или не соответствует действительности, то и остальной материал также не будет заслуживать доверия.

2. Поиск других источников информации Сравнение – один из самых эффективных способов поиска истины. Редко одна и та же недостоверная информация публикуется на нескольких сайтах сразу. Поэтому, если одни и те же данные встречаются в Интернете на совершенно разных ресурсах, то им можно доверять. При этом стоит уделить внимание первоначальному источнику информации. К сожалению, не редки случаи, когда все сайты ссылаются на один и тот же недостоверный источник.

3. Установление использования материала другими источниками Перепечатка и копирование данных с одного сайтам другими сайтами является хорошим знаком, поскольку это означает, что этому источнику доверяют. Чем больше ссылок на исходный материал мы найдем в Интернете, тем выше его авторитет в глазах других ресурсов. Несомненно, это говорит в пользу приведенной информации.

4. Выяснение рейтинга и авторитета сайта Самый простой и действенный способ убедится в правдивости полученной информации, это ознакомится с репутацией сайта, на котором она размещена. Известные ресурсы обычно заслуживают доверия, поскольку трепетно относятся к своему рейтингу и не станут разменивать его на сомнительные сенсации. Узнать о популярности

сайта можно с помощью специальных рейтинговых систем, например через топ «Рамблера» и «Яндекса». Также можно просто вбить название ресурса в любой поисковик и почитать отзывы о нем. Хорошим знаком является наличие у ресурса свидетельства о регистрации СМИ. Онлайн-СМИ несут особую ответственность за любую опубликованную информацию, поэтому стараются избегать непроверенных данных. Кроме того, проверенные данные публикуют официальные сайты, являющиеся первоисточниками.

5. Получение информации об авторе материала Для того чтобы понять, стоит ли доверять какой-либо статье, можно поискать информацию о статусе и компетентности ее автора. Не лишним будет ознакомиться с другими его работами, комментариями и отзывами читателей. Если автор статьи имеет хороший журналистский опыт, почетную должность или научную степень, шансы на правдивость его доводов прилично возрастают. Кроме того, в Интернете могут быть его блоги, страницы социальной сети и прочая информация, которая поможет составить мнение об авторе.

Поиск – это серьезно

Не менее важен грамотный подход к самому процессу поиска информации. Редкий пользователь точно знает сайты, на которых может получить интересующие его данные. Подавляющее большинство людей использует популярные поисковые сервисы, такие как Google, Yandex, Rambler и Mail. Очень многое зависит от поисковой процедуры и формулировки запроса. Любая поисковая система ищет в своей базе данных из миллиарда страниц те, что соответствуют заданным параметрам. Для этого используется так называемая программа индексации. Она распознает текст, связи, и другое содержание страницы, и хранит это в файлах базы данных так, чтобы страница могла быть найдена по ключевым словам. После того, как пользователь делает поисковый запрос, машина ищет нужное слово в своем индексе. Если бы система искала по всему Интернету, то на ответ ей понадобилось бы несколько дней. Поскольку поиск ведется в индексе, многие результаты могут быть устаревшими. Всем известен пример, когда страница уже не существует, а поисковик все еще ее находит и восстанавливает. При этом многие свежие сайты в поисковый результат не попадают. Поэтому если мы не может найти что-либо в одной поисковой системе, имеет смысл поискать в другой.

Подытоживая, можно сделать следующие выводы. Необходимо четко представлять себе, что мы ищем. Правильно сформулированный запрос сэкономит много времени и усилий, а также позволит найти именно то, что нужно. Стоит доверять официальным сайтам и их пресс-релизам. Также заслуживают доверия информационные агентства, научные институты и их исследования. За опубликованные данные несут ответственность онлайн-СМИ. Отдельную категорию составляют материалы, перепечатанные из реальных источников, но доступные в Интернете. Например, учебники и энциклопедические данные. При этом нужно настороженно относиться к таким ресурсам, как Википедия. Информация, опубликованная в ней, вполне может оказаться недостоверной, поскольку доступ к редактированию статей имеет любой желающий. Это может быть, как опытный профессор, так и обыкновенный школьник. Википедия хороша для расширения кругозора, однако ссылаться на нее в серьезной работе весьма опасно. Тоже самое можно сказать и о блогах. Блоггеры, которых называют «гражданскими журналистами», порой располагают очень интересной информацией, которую нельзя найти даже в СМИ. Но при этом часто никто кроме автора блога не может подтвердить достоверность опубликованной информации. Поэтому использовать блоггерские данные нужно осторожно, проверяя их особенно тщательно. Конечно, речь не идет о президентском блоге или «официальных» блогах компаний.

Руководствуясь правилами элементарной логики, подготовленный пользователь сумеет отличить правду от лжи. Однако даже самый искушенный человек может оказаться обманутым. Засилье многочисленных красиво оформленных сайтов мошенников и желтой прессы способно ввести в заблуждение кого угодно. Крайне важно проверять все важные данные, найденные в Интернете, поскольку последствия использования недостоверной информации могут быть весьма печальными.