Безопасное поведение детей в сети Интернет

Какие угрозы встречаются наиболее часто

Угроза заражения вредоносным ПО

Ведь для распространения вредоносного ПО и проникновения в компьютеры используется целый спектр методов. Среди таких методов можно отметить не только почту, компакт-диски, дискеты и прочие сменные носители информации или скачанные из Интернет файлы. Например, программное обеспечение для мгновенного обмена сообщениями сегодня являются простым способом распространения вирусов, так как очень часто используются для прямой передачи файлов. Дети, неискушенные в вопросах социальной инженерии, могут легко попасться на уговоры злоумышленника. Этот метод часто используется хакерами для распространения троянских вирусов.

Какие угрозы встречаются наиболее часто

Доступ к нежелательному содержимому

Ведь сегодня дела обстоят таким образом, что любой ребенок, выходящий в Интернет, может просматривать любые материалы. А это насилие, наркотики порнография, страницы подталкивающие молодежь к самоубийствам, анорексии (отказ от приема пищи), убийствам, страницы с националистической или откровенно фашистской идеологией и многое-многое другое. Ведь все это доступно в Интернет без ограничений. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна содержащие любую информацию, чаще всего порнографического характера.

Какие угрозы встречаются наиболее часто

Контакты с незнакомыми людьми

С помощью чатов или электронной почты. Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. В других случаях это могут быть педофилы, которые ищут новые жертвы. Выдавая себя за сверстника жертвы, они могут выведывать личную информацию и искать личной встречи.

Неконтролируемые покупки

Не смотря на то, что покупки через Интернет пока еще являются экзотикой для большинства из нас, однако недалек тот час, когда эта угроза может стать весьма актуальной.

Угрозы, подстерегающие в Глобальной сети:

Даже случайный клик по всплывшему баннеру или переход по ссылке может привести на сайт с опасным содержимым!

Порнография

Опасна избыточной информацией и грубым, часто извращенным, натурализмом. Мешает развитию естественных эмоциональных привязанностей.

Депрессивные молодежные течения

Ребенок может поверить, что шрамы – лучшее украшение, а суицид – всего лишь способ избавления от проблем.

Угрозы, подстерегающие в Глобальной сети:

Даже случайный клик по всплывшему баннеру или переход по ссылке может привести на сайт с опасным содержимым!

Наркотики

Интернет пестрит новостями о “пользе” употребления марихуаны, рецептами и советами изготовления “зелья”.

Сайты знакомств, социальные сети, блоги и чаты

Виртуальное общение разрушает способность к общению реальному, “убивает” коммуникативные навыки, которые мы невольно приобретаем с самого раннего детства.

Угрозы, подстерегающие в Глобальной сети:

Даже случайный клик по всплывшему баннеру или переход по ссылке может привести на сайт с опасным содержимым!

Секты

Виртуальный собеседник не схватит за руку, но ему вполне по силам “проникнуть в мысли” и повлиять на взгляды на мир

Экстремизм, национализм, фашизм

Все широкие возможности Интернета используются представителями экстремистских течений для того, чтобы заманить в свои ряды новичков.

Интернет это прекрасное место для общения, обучения и отдыха. Но стоит понимать, что как и наш реальный мир, всемирная паутина так же может быть весьма и весьма опасна. Приведем несколько рекомендаций, с помощью которых посещение Интернет может стать менее опасным для ваших детей:

Посещайте Интернет вместе с детьми. Поощряйте ваших детей делиться с вами их успехами и неудачами в деле освоения Интернет;

- *Объясните детям, что если в Интернет что-либо беспокоит их, то им следует не скрывать этого, а поделиться с вами своим беспокойством;*
- *Объясните ребенку, что при общении в чатах, использовании программ мгновенного обмена сообщениями (типа ICQ, Microsoft Messenger и т.д.), использовании он-лайн игр и других ситуациях, требующих регистрации, нельзя использовать реальное имя, помогите вашему ребенку выбрать регистрационное имя, не содержащее никакой личной информации;*

- *Объясните ребенку, что нельзя выдавать свои личные данные, такие как домашний адрес, номер телефона и любую другую личную информацию, например, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т.д.;*
- *Объясните своему ребенку, что в реальной жизни и в Интернет нет разницы между неправильными и правильными поступками;*
- *Научите ваших детей уважать собеседников в Интернет. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково в Интернет и в реальной жизни;*
- *Скажите им, что никогда не стоит встречаться с друзьями из Интернет. Ведь люди могут оказаться совсем не теми, за кого себя выдают;*

•Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернет – правда. Приучите их спрашивать о том, в чем они не уверены;

•Не забывайте контролировать детей в Интернет с помощью специального программного обеспечения. Это поможет вам отфильтровывать вредоносное содержание, выяснить, какие сайты на самом деле посещает ваш ребенок и что он там делает.

В подтверждение этому сайт «Ребенок в сети» (http://www.detionline.ru) опубликовал следующие данные:

1. 25% пятилетних детей используют Интернет.
2. В 2004 году Интернетом пользовалось больше детей, чем взрослых.
3. По данным исследования, опубликованного в 2002 году в Испании Агентством защиты детей (Child Protection Agency), 44% детей, регулярно использующих Интернет, один раз подвергались сексуальным домогательствам при виртуальном общении, 11% подверглись этому несколько раз. В других случаях воздействие может принимать форму оскорблений со стороны других Интернет-пользователей или почтовых сообщений с оскорбительным содержанием.
   Особо тревожные данные: 14,5% детей, принявших участие в опросе, назначали встречи с незнакомцами через Интернет. 10% из них ходили на встречи в одиночку, а 7% никому не сообщили, что с кем-то встречаются.
4. 28% детей посещают порнографические веб-страницы.
5. 50% детей выходят в Интернет одни. В связи с этим возникает вопрос: «Какие меры предосторожности нужно предпринимать детям, чтобы не попасть в лапы Интернет-преступников?».

Вот рекомендации специалистов:

- Никогда не скачивать изображения из неизвестного источника.
- Использовать фильтры электронной почты.
- Немедленно сообщать взрослым обо всех случаях в Интернете, которые вызвали смущение или испуг.
- Использовать нейтральное в половом отношении экранное имя, не содержащее сексуальных намеков и не выдающее никаких личных сведений.
- Никогда и никому в Сети не сообщать информацию о себе (включая возраст и пол) или о семье.
- Прекращать любые контакты по электронной почте, в системе обмена мгновенными сообщениями (посредством программ типа ICQ) или в чатах, если кто-нибудь начинает задавать вопросы личного характера или содержащие сексуальные намеки.

Что могут сделать родители?

- *Расскажите своим детям о существовании злоумышленников и о потенциальных опасностях глобальной сети.*
- *Маленьким детям не следует пользоваться чатами — слишком велика опасность. Только когда ваш ребенок подрастет, можно разрешить общаться там, где есть контроль над сообщениями (или, говоря компьютерным языком, «модерация»). Вообще имеет смысл, чтобы дети общались только в таких чатах.*
- *Если ваши дети пользуются чатами, вам следует знать, какими именно и с кем они там беседуют. Лично посетите чат, чтобы проверить, на какие темы ведутся дискуссии.*
- *Внушите детям, что никогда нельзя покидать общий чат. Многие сайты имеют «приватные комнаты», где пользователи могут вести беседы наедине — у администраторов нет возможности читать эти беседы. Такие «комнаты» часто называют «приватом».*

Что могут сделать родители?

- *Пока дети маленькие, лучше, чтобы они пользовались общим электронным адресом семьи, а не своим собственным. То есть у вас должен быть доступ.*
- *Объясните детям, что никогда не следует отвечать на мгновенные сообщения или письма по электронной почте, поступившие от незнакомцев.*
- *Накажите детям, чтобы они никогда не отвечали на мгновенные сообщения или письма по электронной почте, поступившие от незнакомцев.*
- *Если, несмотря на все меры предосторожности, ваши дети познакомились в Интернете со злоумышленником, не вините их. Вся полнота ответственности всегда лежит на правонарушителе. Предпримите решительные действия для прекращения дальнейших контактов ребенка с этим лицом.*

- *Много полезных советов по компьютерной безопасности для детей разных возрастов и родителей можно найти на сайте Компании Microsoft по адресу: http://www.microsoft.com/rus/athome/security/children/backtoschool.mspx.*

Советы родителям

Безопасные пароли

Одним из способов является придумать известное предложение и взять из каждого слова первые буквы. Например, «Наш Сергей родился в 99», при этом с использованием английского алфавита получится пароль YChd99. Просто запомнить, сложно догадаться. Никогда не создавайте пароль, который может отгадать друг (например, кличка домашнего животного).

Фильтр поиска MSN

В Интернете содержатся материалы, неуместные для детей. Большую часть таких материалов можно заблокировать с помощью ряда фильтров. Важно понимать, что такая технология не является единственным способом защиты детей от неуместных материалов в Интернете.

Безопасное пространство

Самым безопасным способом путешествия по просторам Интернета для детей является создание безопасного пространства или области, в которой разрешен просмотр сайтов, одобренных взрослым человеком. Для разрешения детям доступа к определенным безопасным сайтам можно использовать параметры обозревателя. В этом случае, если ребенку необходимо посетить новый сайт, сначала необходимо добавить его адрес в список разрешенных сайтов. В операционной системе Windows XP можно легко создавать безопасные пространства.

Для ребенка необходимо создать персональную учетную запись пользователя в операционной системе. При этом для ребенка определяются права доступа и параметры обозревателя Интернета.

Программы фильтрации

Программы фильтрации предоставляют функции ограничения веб-сайтов на основе содержимого. Это означает, что программой блокируется доступ к сайтам, содержащим материалы, которые определены как опасные (порнография, насилие и т.д.).

Ограничение входящих контактов

С помощью технологии фильтров и блокировки можно ограничить список собеседников, с которым дети общаются через Интернет. Для получения более подробной информации см. страницы в разделах Использование электронной почты и Программы мгновенного обмена сообщениями.

Журнал просмотренных веб-страниц

С помощью функции журнала просмотренных веб-страниц в обозревателе Интернета можно просмотреть веб-сайты, посещенные другими пользователями за последнее время (хотя журнал просмотренных веб-страниц легко удалить).

Совет

Что следует делать, если ребенок увидел в Интернете неприятные или неуместные материалы?

– Не реагируйте слишком остро: ребенок не должен чувствовать излишнего смущения, чтобы он мог свободно говорить о подобных случаях в будущем.

– Акцентируйте внимание ребенка на том, что это не его вина.

– Удалите любые следы, оставшиеся от неуместного материала, включая ссылки из кэш-памяти обозревателя, файлы cookie и журнал просмотренных веб-страниц.

– Поговорите с ребенком о том, как избежать подобных ситуаций в будущем, включая использование детских поисковых модулей и удаление сообщений электронной почты от неизвестных людей.

Использование Интернета является безопасным, если выполняются три правила:

Защитите свой компьютер

- Регулярно обновляйте операционную систему.
- Используйте антивирусную программу.
- Применяйте брандмауэр.
- Создавайте резервные копии важных файлов.
- Будьте осторожны при загрузке новых файлов.

Защитите себя в Интернете

- С осторожностью разглашайте личную информацию.
- Думайте о том, с кем разговариваете.
- Помните, что в Интернете не вся информация надежна и не все пользователи откровенны.

Соблюдайте правила

- Закону необходимо подчиняться даже в Интернете.
- При работе в Интернете не забывайте заботиться об остальных так же, как о себе.

Наиболее важным является обеспечение безопасности личной информации на собственном компьютере, что означает защиту от вирусов и обновление программного обеспечения. Что касается детей, повысить уровень защиты данных можно путем использования настроек фильтра и параметров фильтрации содержимого, которые доступны во многих программах.