Информационная безопасность пользователей интернета. Профилактика основных интернет-рисков и борьба с ними

Учитель информатики МБОУ СОШ №100

Старцев Борис Александрович

Вместо предисловия…

Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29 декабря 2010 года № 436-ФЗ устанавливает правила медиа-безопасности детей при обороте на территории России продукции средств массовой информации, печатной, аудиовизуальной продукции на любых видах носителей, программ для ЭВМ и баз данных, а также информации, размещаемой в информационно-телекоммуникационных сетях и сетях подвижной радиотелефонной связи.

Согласно российскому законодательству информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию.

Вопросы

- Кто и для чего создает вредоностные программы?
- Какие виды угроз существуют?
- Как оградить ребенка от интернет-угроз?
- Что делать, если ребенок уже столкнулся с какой-либо интернет-угрозой?

Кто и для чего создает вредоносные программы?

Компьютерные хулиганы – вандалы, встречающиеся в киберпространстве, создают программы лишь для того, чтобы нанести вред компьютеру ребенка, как правило, это тщеславные студенты, неопытные юнцы, прибегающие к помощи интернета, то также встречаются и профессиональные разработчики.

Мелкое воровство – молодые вирусописатели, целью которых является получение выгоды использования определенных сервисов или услуг (кража логинов и паролей, например, от социальных сетей, в которых так часто сидят наши дети).

Киберпреступники – наиболее опасная категория вирусописателей, хакеры-одиночки или группа хакеров, которые создают вредоносные программы, чтобы использовать их в криминальных целях (кража кодов доступа к банковским счетам, шантаж, нелегальное использование ресурсов компьютера «жертвы» для дальнейших сетевых атак).

Серый бизнес – самая опасная категория вирусописателей, поскольку действует на грани закона, а зачастую, вне его. Целью является заманить ребенка на платные веб-ресурсы или предложить фальшивую программу, которая, якобы должна помочь оптимизировать работу компьютера. Для достижения своей цели, используют хакерские технологии получения доступа к компьютеру без ведома ребенка и что опаснее, без противодействия антивирусного ПО.

Классификация угроз

Условно все угрозы можно разделить на следующие типы:

- Компьютерный вирус (червь)
- Троянская программа
- Adware, Pornware, Riskware
- Спам и фишинг
- Интернет угрозы
- Мобильные угрозы

Компьютерный вирус (червь)

Компьютерный вирус и компьютерный червь — это вредоносные программы, которые способны воспроизводить себя на компьютерах или через компьютерные сети. При этом ребенок не подозревает о заражении своего компьютера. Так как каждая последующая копия вируса или компьютерного червя также способна к самовоспроизведению, заражение распространяется очень быстро. Существует очень много различных типов компьютерных вирусов и компьютерных червей, большинство которых обладают высокой способностью к разрушению.

Троянская программа

Троянские программы — это вредоносные программы, выполняющие несанкционированные пользователем действия. Такие действия могут включать:

- удаление данных;
- блокирование данных;
- изменение данных;
- копирование данных;
- замедление работы компьютеров и компьютерных сете

В отличие от компьютерных вирусов и червей троянские программы не способны к самовоспроизведению

Adware, Pornware, Riskware

Категория Adware, Pornware и Riskware включает легально разработанные программы, которые в определенных случаях могут представлять особую опасность для детей (действуя так же, как шпионское программное обеспечение). Хотя многие из таких программ, вероятно, разработаны и распространяются легальными компаниями, они могут иметь функции, которые используются некоторыми создателями вредоносных программ во вредоносных или незаконных целях.

Спам и фишинг

- Спам — это электронный эквивалент бумажной рекламы, которую бросают в ваш почтовый ящик. Однако спам не просто надоедает и раздражает. Он опасен, особенно если является частью фишинга. Спам в огромных количествах рассылается по электронной почте спамерами и киберпреступниками цель которых:
- выудить деньги у некоторого количества получателей, ответивших на сообщение;
- провести фишинговую атаку, чтобы обманным путем получить пароли, в том числе и от социальных сетей, где так часто сидит ребенок;
- распространить вредоносный код на компьютерах получателей

Интернет угрозы

Под интернет-угрозами понимаются вредоносные программы, оторые могут представлять опасность во время работы детей в нтернете. Существует ряд интернет-угроз, которые проникают на омпьютер пользователя через браузер.

Основным инструментом заражений через браузер являются ксплойты. Они открывают киберпреступникам дорогу для аражения компьютера:

- если на компьютере не установлен продукт, обеспечивающий защиту от интернет-угроз (комплексное антивирусное решение класса Internet Security);
- если компьютер использует популярную операционную систему или приложение, которое является уязвимым, потому что пользователь не загрузил последние обновления или новое исправление еще не выпущено вендором программного обеспечения.

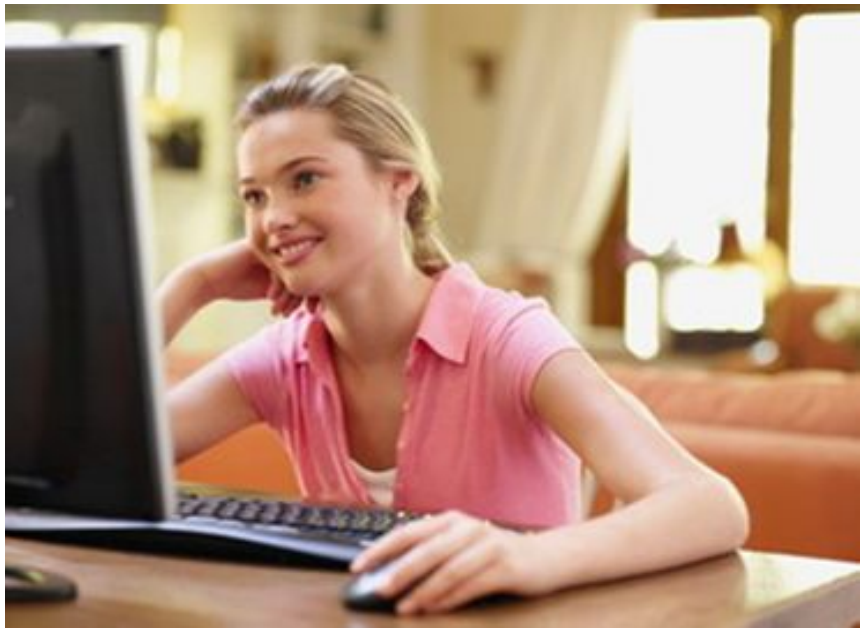
Мобильные угрозы

Поскольку все больше детей используют смартфоны и планшеты для просмотра веб-страниц, общения в социальных сетях, совершения покупок и банковских операций в интернете, киберпреступники все чаще атакуют мобильные устройства, используя при этом новые угрозы для смартфонов и мобильных устройств.

Наиболее распространенные вредоносные объекты, обнаруженные на смартфонах, можно разделить на три основные группы:

- SMS-троянцы;
- рекламные модули;
- эксплойты для получения доступа уровня root к смартфонам.

Как оградить ребенка от интернет-угроз?



- Одним из важных моментов защиты ребенка от интернет угроз, является контентная фильтрация интернет ресурсов. Школа должна позаботится о безопасном пребывании детей в информационном пространстве. В МБОУ СОШ № 100 существует контентная фильтрация на базе Kaspersky Security Center. Главная идея такой фильтрации заключается в том, что «подозрительные» сайты система не пропустит, т.е. ребенок будет огражден от нежелательного контента. Важным преимуществом такой системы является не только запрет, но и мониторинг, на основании которого можно посмотреть с какого компьютера и на какой ресурс пытался зайти учащийся.
- Пользуйтесь на компьютере только подлинным ПО, убедитесь, что на компьютере установлены последние обновления (пакеты) безопасности для ОС, а также антивирусные базы.
- Используйте на компьютере не просто антивирус, а систему класса (Total Security или Internet Security), в которой помимо традиционного сканера на вирусы, существует защита от других видов атак + родительский контроль, позволяющий родителям самим ограничивать ребенка от нежелательного контента.

Профилактика основных интернет-рисков и борьба с ними

Дети и подростки — активные пользователи интернета. С каждым годом сообщество российских интернет-пользователей молодеет. Дети поколения Рунета растут в мире, сильно отличающемся от того, в котором росли их родители, учителя, да и в принципе взрослые люди. Одной из важнейших координат развития учащихся становятся инфо-коммуникационные технологии и, в первую очередь, интернет. Между тем, помимо огромного количества возможностей, интернет несет и множество рисков. Зачастую дети и подростки в полной мере не осознают все возможные проблемы, с которыми они могут столкнуться в сети. Сделать пребывание детей в интернете более безопасным, научить их ориентироваться в киберпространстве — важная задача как для родителей, так и для нас – учителей информатики.

Что делать, если ребенок уже столкнулся с какой-либо интернет-угрозой?

- Установите положительный эмоциональный контакт с ребенком, постарайтесь расположить его к разговору о том, что произошло. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен вам доверять и понимать, что вы хотите разобраться в ситуации и помочь ему, но ни в коем случае не наказать.
- Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети) или он попал в неприятную ситуацию (потратил деньги в результате интернет-мошенничества и пр.), постарайтесь его успокоить и вместе разберитесь в ситуации. Выясните, что привело к данному результату – непосредственно действия самого ребенка, недостаточность вашего контроля или незнание ребенком правил безопасного поведения в интернете.

Что делать, если ребенок уже столкнулся с какой-либо интернет-угрозой?

- Если ситуация связана с насилием в интернете в отношении ребенка, то необходимо узнать информацию об обидчике, историю их взаимоотношений, выяснить, существует ли договоренность о встрече в реальной жизни и случались ли подобные встречи раньше, узнать о том, что известно обидчику о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т. п.). Объясните и обсудите, какой опасности может подвергнуться ребенок при встрече с незнакомцами, особенно без свидетелей.
- Соберите наиболее полную информацию о происшествии – как со слов ребенка, так и с помощью технических средств. Зайдите на страницы сайта, где был ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию – в дальнейшем это может вам пригодиться для обращения в правоохранительные органы.

Памятка умный пользователь интернета

- **Ведет себя вежливо и не обижает других**
- **Покидают нехорошие веб-сайты**
- **Хранят свой пароль в тайне**
- **Рассказывают родителям о своих проблемах и пользуются их поддержкой**
- **Знают, что могут быть легко обмануты и не сообщают свои реальные имена, адреса и номера телефонов**

Подводим итоги…

Решение задачи по обеспечению безопасности при использовании компьютера и интернета детьми требует комплексного подхода, решения множества психолого-педагогических вопросов. Школа должна играть одну из ключевых ролей в обучении детей безопасному использованию интернет-технологий. Помимо выполнения очевидных мер безопасности (установка антивирусных программ, брандмауэров, фильтров, ограничений по времени) необходима разработка и реализация правил электронной безопасности, которые требуют привлечения широкого спектра заинтересованных лиц: директора школы, классных руководителей, преподавателей информационных технологий, самих учащихся и их родителей, поставщико услуг интернета.

Давайте вместе сделаем пребывание наших детей в сети безопасным, увлекательным и интересным!

Используемые источники

- Бесплатная всероссийская служба «**Дети Онлайн**»
  http://detionline.com
- Статья кандидата психологических наук **Крылова Т.А**. «Информационная безопасность детей в использовании Интернет-ресурсов»
- Аналитический центр **Ati-Malware.ru**
  http://anti-malware.ru
- **Kaspersky Security Bulletin** – Все об интернет безоп
  http://securelist.ru
- **Dr.Web** – Комплексная защита от интернет угроз
  http://drweb.ru