Тема: Опасности, с которыми дети могут столкнуться в сети Интернет

Составитель – педагог дополнительного образования Франчук С. Г.

Слайд 1. Цель: информирование родителей об опасностях Интернета.

Задачи:

- познакомить родителей школьников с распространенными Интернет-угрозами;
- предложить рекомендации по нейтрализации угроз, поступающих из сети Интернет.

Оборудование: компьютер, мультимедийная презентация.

Слайд2

Добрый день, уважаемые родители!

Сегодня мы с вами обсудим, какие опасности подстерегают нас и наших детей, кто может представлять угрозы в сети и кто такие интернет-мошенники, как уберечься от недостоверной информации и не стать самому нарушителем. Вам будут предложен ряд рекомендаций, которые помогут организовать безопасную работу в сети интернет, мы поговорим о наиболее часто встречающихся угрозах, об угрозе заражения вредоносным ПО, об угрозах которые могут привести к потере денег, также мы поговорим о том, как предотвратить доступ к агрессивному, неприятному или незаконному содержанию, как избежать угроз при контакте с незнакомыми людьми. Вы можете сами того не ведая совершать преступления в сети, например нарушать авторские права, участвовать в сетевых атаках или распространения спама.

Слайд 3. Давайтепоговорим об угрозе заражения компьютерными вирусами.

Компьютерные вирусы- небольшие программы которые распространяются с компьютера на компьютер и вмешиваются в работу операционной системы. Вирусы могут распространиться на компьютере и уничтожить все данные (фотографии, видео, файлы с важной информацией). Проще всего вирусы распространяются во вложениях электронной почты, поэтому очень важно никогда не открывать вложения, если вы не ожидали их получить или не знаете, кто их отправил. Вирусы могут распространяться под видом картинок, поздравительных открыток, звуковых или видеофайлов, их можно загрузить из интернета вместе с нелицензионным программным обеспечением или другими файлами и программами.

Слайд 4

Правило.Перед загрузкой файлов необходимо какможно надежней защититься от нежелательных программ. Установите и регулярно обновляйте программы для защиты компьютера. Настройте антивирусную программу

для автоматической проверки всех загружаемых файлов и вложений электронной почты перед их открытием. Установите и запустите приложение для обнаружения и удаления программ-шпионов.

Слайд 5Нежелательная почта или СПАМ.

Спам (англ. spam) — сообщения, массово рассылаемые людям, не дававшим согласие на их получение. В первую очередь, термин «спам» относится к электронным письмам . Эта аббревиатура связана с говяжьими консервами, которые их создатель додумался очень активно рекламировать: рассыпать листовки по площадям, присылать всем по почте. Поэтому такую рекламу и назвали в честь этих консервов.

Несмотря на то, что свои логин и пароль вы храните в секрете, сам по себе ваш адрес электронной почты не является секретом. Существуют различные системы, которые с помощью специальных роботов находят в сети электронные адреса с целью рассылки информации или мошеннических предложений. Такие письма называются СПАМ. При получении письма, содержание которого не имеет к вам никакого отношения, тем не менее, вы можете открыть письмо и прочитать его. Часто это письма рекламного характера. Однако ни в коем случае не нажимайте никакие ссылки, расположенные в таких письмах. Иначе впоследствии вас просто завалят спамом. Часто к таким письмам добавлены вложения, в которых могут содержаться вирусы.

Слайд 6

Правила. Просто игнорируйте предложение или отправьте письмо в папку Спам и просто периодически удаляйте все из нее.

Слайд 7. Агрессивная, неприятная и незаконная информация.

Речь пойдет о материалах, текстах картинках аудио и видеофайлах, которые содержат насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анарексии, суицида, азартных игр, наркотических вещества. Столкнуться сними можно практически везде - это и сайты и соцсети, блоги, торренты, видеохостинги. Независимо от желания пользователя на многих сайтах отображаются всплывающие окна, содержащие подобную информацию. Зачастую подобный материал может прийти от незнакомца по почте. В сети человек можете столкнуться с материалами, которые являются просто незаконными - изготовление, продажа, употребление наркотиков, разжигание расовой или религиозной ненависти, а также ненависти или агрессивного поведения по отношению к группе людей, отдельной личности или животных, азартные игры и т.д. В нашей стране существуют различные виды наказания за распространение такого рода информации. В российском законодательстве

есть возможность в соответствии с УК привлечь к административной или уголовной ответственности за распространение подобного негативного контента владельцев сайтов, а также авторов таких электронных текстов и видеопродукции. В сети можно встретить материалы, которые противоречат принятым нормам морали, но они не подпадают под действие УК однако могут оказывать негативное воздействие на психику ребенка, который с ними столкнется. Помните, информация на страницах сайтов может быть направлена на то, чтобы управлять нашим сознанием и сознанием наших детей, а также влиять на наши действия.

Слайд 8

Правила.Основное правило – стараться не посещать сайты такого содержания, поставить запрет на адрес. А что касается детей, им необходимо объяснить, что далеко не все что можно увидеть в интернете - правда.

Помимо нежелательной информации, Интернет представляет собой еще и **опасность быть обманутыми.**

Слайд 9

Онлайн-мошенничество. При всякой деятельности в сети интернет нужно соблюдать правила безопасности, чтобы не попасться на удочку мошенника, которых в сети не меньше чем в реальной жизни. Например, фишинг. Это хищение личных данных- номера кредитных карт родителей, пароли личных данных. Получали Вы предложения о составлении гороскопа, предложения о легком заработке денег, предоставлении ссылки для скачивания, где всего лишь надо заплатить 50-100 рублей (показав номер карты или мобильного телефона). Здесь можно говорить о доверчивости каждого конкретного человека (если говорить о взрослом контингенте), а что говорить о доверчивости детей? Именно дети и подростки, выходя в Сеть, попадают в зону риска.

Слайд 10

Правила. Научите ребенка не отвечать на подозрительные рассылки. Если Вы показываете в сети кредитную карту или свои паспортные данные, убедитесь в надежности этого сайта, не отправляйте по электронной почте свои паспортные и другие личные данные.

Слайд 11

В Сети ребенок может столкнуться с одной из наиболее серьезных угроз — педофилией.

Местами повышенной опасности признаны Интернет-чаты, где, с точки зрения экспертов, риск попасть на удочку педофилов — самый высокий. Общаясь в своих чатах, дети и подростки абсолютно уверены, что говорят с

ровесниками. Им не приходит в голову, что взрослый человек может общаться на их языке, отлично разбирается в телепрограммах, которые они смотрят, одежде, которую они носят, и т.д. Нередко дети соглашаются дать собеседнику по чату номер своего мобильного телефона, домашний адрес и даже встретиться с ним.
Поэтому именно родители, должны предупредить ребенка об опасности стать жертвой педофила, заставить его дважды подумать о том, кем на самом деле может являться его собеседник в Интернете и, тем более, проявить меры предосторожности при попытке встретиться со знакомыми из Сети. Очень часто госструктуры контролируют только какой-то один фронт опасного содержания в Интернете, например терроризма, а доступ к сайтам, экстремистского и порнографического содержания, должным образом не контролируется.

Правила. При общении научите ребенка использовать только имя или лучше псевдоним (ник) при общении в сети. Номер телефона, свой адрес, место учебы нельзя сообщать. Неразрешайте пересылать детям свои фотографии, без контроля взрослых дети не должны встречаться с людьми, знакомство с которыми завязалось в сети.

Слайд 12

Как же обезопасить работу ребенка в сети:

1.Правильно настройте браузер, специальную программу, предназначенную для просмотра веб-сайтов (InternetExplorer, GoogleChrome, MozillaFirefox**)** в котором работает ребенок.

Слайд 13

2.Контролируйте посещений сайтов через вкладку«Журнал» в браузере.

Слайд 14

3.Установите на компьютер антивирусное программное обеспечение.

Слайд 15

4.Установите на компьютер программу интернет-фильтр.

5.Нежелательную почта просто игнорируйте или отправьте письмо в папку «Спам» и периодически удаляйте все из нее.

6. Стараться не посещать сайты, содержащие агрессивную, неприятную и незаконную информация, поставить запрет на этот адрес.

7.Не разрешайте пересылать детям свои фотографии, без контроля взрослых дети не должны встречаться с людьми, знакомство с которыми завязалось в сети.

Слайд 16-20

Рекомендуем Вам программу Интернет-цензор. Эта программа создана для всех заботливых родителей. Именно поэтому она бесплатна, как и

бесплатны обновления к ней. Скачайте Интернет Цензор и используйте эту программу для того, чтобы защитить своих детей. Интерфейс программы очень простой: настраивается уровень фильтрации, создаются списки запрещенных и разрешенных сайтов и выполняются общие настройки программы. Проект «Интернет Цензор» разработан при содействии Фонда поддержки развития общества «Наши дети». Главная задача программы - сделать пребывание детей и подростков в Интернете безопасным, оградив их от вредных ресурсов.

Теперь вы, уважаемые родители,понимаете, насколько важно со всей серьезностью отнестись к вопросу безопасности и защищенности вашихдетей от негативного воздействия на нихинтернет-угроз. Внимательно присмотритесь к обычной жизни, есть возрастные ограничения на просмотр фильмов (и по телевидению, и в кинотеатрах), ограничение на покупку определенных товаров (книг, журналов). В то же время в Интернете информация может висеть в общем доступе, и ее может увидеть любой желающий независимо от возраста.

Список использованных источников:

1.Статья «Интернет-угрозы для ребенка при работе в сети Интернет» Авторы:Фомина Е.Ю., Шубинский М.И.http://www.securrity.ru/articles/1269-internet-ugrozy-dlya-rebenka-pri-rabote-v-seti-internet.html
2. «Подросток и закон». Интернет-угрозы.
http://podrostok.edu.yar.ru/safety/index.html
3. «Интернет цензор» http://icensor.ru/soft/
4.Инструкция по установке программы «Интернет Цензор»http://icensor.ru/support/video/