**ВСЕРОССИЙСКИЙ**

**УРОК БЕЗОПАСНОСТИ**

**ШКОЛЬНИКОВ В СЕТИ**

**ИНТЕРНЕТ**



**Тема: Единый урок «Безопасный Интернет»**

**Цель урока:**

Познакомить учащихся с преимуществами сети Интернет, скрытыми и открытыми угрозами Интернета, классификации интернет угроз;

Сформировать понятия Интернета; Научить учащихся критически относиться к информационной продукции, распространяемой в сети Интернет; Уметь отличать достоверные сведения от недостоверных, вредную информацию от безопасной; Распознавать признаки злоупотребления неопытностью и доверчивостью учащихся, попытки вовлечения их в противоправную деятельность.

**Оборудование:** компьютер с проектором или телевизор с разъёмом USB, видеоролик, буклеты, смайлики.

**Ход урока**

**1. Организационный момент (приветствие учащихся начальной школы, основной и средней школы).**

**2. Мотивационное начало урока**

Тема нашего урока “Безопасность в Интернете”.

**Безусловные преимущества использования Интернет**

В настоящее время Интернет стал неотъемлемой частью повседневной жизни, бизнеса, политики, науки и образования. Использование Интернета дома и в образовательных учреждениях позволяет повысить эффективность обучения, а так же получать свежие новости в интересующей области не только родителям и педагогам, но и учащимся, в том числе школьникам.

**Скрытые и открытые угрозы Интернет**

Однако бурное развитие Интернета несет также существенные издержки. Современная научно-образовательная информационная среда характеризуется большим количеством образовательных ресурсов с неструктурированной и мало того, еще и не всегда достоверной информацией. Объем подобных ресурсов растет в геометрической прогрессии. Таким образом, неуклонно возрастает потребность в обеспечении эффективного использования информационных научно-образовательных ресурсов. Кроме того, наряду с полезной и необходимой информацией пользователи сталкиваются ресурсами, содержащими неэтичный и агрессивный контент. Порнография, терроризм, наркотики, националистический экстремизм, маргинальные секты, неэтичная реклама и многое другое — яркие примеры контента, с которым могут соприкоснуться дети и подростки. Бесконтрольное распространение нежелательного контента противоречит целям образования и воспитания молодежи. Отказываться от благ информационных технологий бессмысленно, но бесконтрольный доступ детей к Интернету может привести к необратимым последствиям.

1. ***Установите комплексную систему защиты.***

Установка обычного антивируса – вчерашний день. Сегодня актуальны так называемые «комплексные системы защиты», включающие в себя антивирус, файрволл, антиспам-фильтр и еще пару-тройку модулей для полной защиты вашего компьютера. Новые вирусы появляются ежедневно, поэтому не забывайте регулярно обновлять базы сигнатур: лучше всего настроить программу на автоматическое обновление.

1. ***Будьте осторожны с электронной почтой***

Не стоит передавать какую-либо важную информацию через электронную почту. Установите запрет открытия вложений электронной почты, поскольку многие вирусы содержатся во вложениях и начинают распространяться сразу после открытия вложения. Программы Microsoft Outlook и Windows Mail помогают блокировать потенциально опасные вложения.

1. ***Пользуйтесь браузерами Mozilla Firefox, Google Chrome и Apple Safari.***Большинство червей и вредоносных скриптов ориентированы под Internet Explorer и Opera. В рейтинге популярности лидирует IE, но лишь потому, что он встроен в Windows. Браузер Opera очень популярен в России из-за ее призрачного удобства и очень большого числа настроек. Уровень безопасности имеет ряд недостатоков как у одного, так и у второго браузера, поэтому лучше ими не пользоваться вовсе.
2. ***Обновляйте операционную систему Windows.***

Постоянно обновляйте операционную систему Windows. Корпорация Microsoft периодически выпускает специальные обновления безопасности, которые могут помочь защитить компьютер. Эти обновления могут предотвратить вирусные и другие атаки на компьютер, закрывая потенциально опасные точки входа.

1. ***Не отправляйте SMS-сообщения.***

Сейчас очень популярны сайты, предлагающие доступ к чужим SMS и распечаткам звонков, также очень часто при скачивании файлов вам предлагают ввести свой номер, или внезапно появляется блокирующее окно, которое якобы можно убрать с помощью отправки SMS.

При отправке SMS, в лучшем случае, можно лишиться 300-600 рублей на счету телефона – если нужно будет отправить сообщение на короткий номер для оплаты, в худшем – на компьютере появится ужасный вирус.

Поэтому никогда не отправляйте SMS-сообщения и не вводите свой номер телефона на сомнительных сайтах при регистрации.

1. ***Пользуйтесь лицензионным ПО.***

Если вы скачиваете пиратские версии программ или свеженький взломщик программы, запускаете его и сознательно игнорируете предупреждение антивируса, будьте готовы к тому, что можете поселить вирус на свой компьютер. Причем, чем программа популярнее, тем выше такая вероятность.

Лицензионные программы избавят Вас от подобной угрозы!

1. ***Используйте брандмауэр.***

Используйте брандмауэр Windows или другой брандмауэр оповещают о наличии подозрительной активности при попытке вируса или червя подключиться к компьютеру. Он также позволяет запретить вирусам, червям и хакерам загружать потенциально опасные программы на компьютер.

1. ***Используйте сложные пароли.***

Как утверждает статистика, 80% всех паролей — это простые слова: имена, марки телефона или машины, имя кошки или собаки, а также пароли вроде 123. Такие пароли сильно облегчают работу взломщикам. В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти символов — два-четыре часа, но чтобы взломать семисимвольный пароль, потребуется два-четыре года. Лучше использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки.

1. ***Делайте резервные копии.***

При малейшей угрозе ценная информация с вашего компьютера может быть удалена, а что ещё хуже – похищена. Возьмите за правило обязательное создание резервных копий важных данных на внешнем устройстве – флеш-карте, оптическом диске, переносном жестком диске.

1. ***Функция «Родительский контроль» обезопасит вас.***

Для детской психики Интернет – это постоянная угроза получения психологической травмы и риск оказаться жертвой преступников.

Не стремитесь утаивать от родителей круг тем, которые вы обсуждает в сети, и новых Интернет-знакомых, это поможет вам реально оценивать информацию, которую вы видите в сети и не стать жертвой обмана.

Соблюдая эти не сложные правила, вы сможете избежать популярных сетевых угроз.

***Школьникам младших классов***

**Если ты любишь сидеть в Интернете, запомни эти правила безопасности!**

|  |  |
| --- | --- |
| Если что-то непонятно  страшно или неприятно, Быстро к взрослым поспеши, Расскажи и покажи. | Как и всюду на планете, Есть опасность в интернете. Мы опасность исключаем, Если фильтры подключаем. |
| Как и всюду на планете, Есть опасность в интернете. Мы опасность исключаем, Если фильтры подключаем. | Злые люди в Интернете Расставляют свои сети. С незнакомыми людьми Ты на встречу не иди! |
| С грубиянами в сети Разговор не заводи. Ну и сам не оплошай - Никого не обижай. | Чтобы вор к нам не пришёл, И чужой нас не нашёл, Телефон свой, адрес, фото В интернет не помещай И другим не сообщай. |

***Школьникам средних классов***

**Вы должны это знать:**

* При регистрации на сайтах, старайтесь не указывать личную информацию, т.к. она может быть доступна незнакомым людям. Так же, не рекомендуется размещать свою фотографию, давая, тем самым, представление о том, как вы выглядите, посторонним людям.
* Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть ваш разговор, т.к. он может быть записан.
* Нежелательные письма от незнакомых людей называются «Спам». Если вы получили такое письмо, не отвечайте на него. В случае, если Вы ответите на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылась вам спам.
* Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.
* Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя в вашем отношении неподобающим образом, сообщите об этом.
* Если вас кто-то расстроил или обидел, расскажите все взрослому.

**Физкультминутка (1 мин)**

Но сначала, мы немножко отдохнем и проведем физкультминутку.

Мы все вместе улыбнемся,

Подмигнем слегка друг другу,

Вправо, влево повернемся

И кивнем затем по кругу.

Все идеи победили,

Вверх взметнулись наши руки.

Груз забот с себя стряхнули

И продолжим путь науки.

Итак, как же бороться с сетевыми угрозами?

***Школьникам старших классов***

**Вы должны это знать:**

* Не желательно размещать персональную информацию в Интернете.

Персональная информация — это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и фотографии вас, вашей семьи или друзей.

* Если вы публикуете фото или видео в интернете — каждый может посмотреть их.
* Не отвечайте на Спам (нежелательную электронную почту).
* Не открывайте файлы, которые прислали неизвестные Вам людей. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.
* Не добавляйте незнакомых людей в свой контакт лист в IM (ICQ, MSN messenger и т.д.)
* Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.
* Если рядом с вами нет родственников, не встречайтесь в реальной жизни с людьми, с которыми вы познакомились в Интернете. Если ваш виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к вашей заботе о собственной безопасности!
* Никогда не поздно рассказать взрослым, если вас кто-то обидел.

**Учителям и преподавателям**

***Чтобы помочь учащимся, Вы должны это знать:***

* Подготовьтесь. Изучите технику безопасности в Интернете, чтобы знать виды Интернет—угроз, уметь их распознать и предотвратить. Выясните, какими функциями обладают компьютеры подопечных, а так же какое программное обеспечение на них установлено.
* Прежде чем позволить ребенку работу за компьютером, расскажите ему как можно больше о виртуальном мире, его возможностях и опасностях.
* Не позволяйте детям самостоятельно исследовать Интернет-пространство, они могут столкнуться с агрессивным контентом.
* Выберите интересные ресурсы и предложите детям изучить их вместе.
* Убедитесь, что на компьютерах установлены и правильно настроены средства фильтрации контента, спама и антивирусы.

***Использование Интернета является безопасным, если выполняются три основные правила.***

***1. Защитите свой компьютер***

Регулярно обновляйте операционную систему.

Используйте антивирусную программу.

Применяйте брандмауэр.

Создавайте резервные копии важных файлов.

Будьте осторожны при загрузке содержимого.

***2. 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.

***3. Соблюдайте правила***

Закону необходимо подчиняться даже в Интернете.

При работе в Интернете не забывайте заботиться об остальных так же, как о себе.

**Каждому участнику СМАЙЛИК и памятка**

**Литература:**

Ссылка на источник:

http://detionline.com/

http://content-filtering.ru – Интернет СМИ «Ваш личный Интернет»;

http://www.rgdb.ru – Российская государственная детская библиотека.

Квест Сетевичок. Единый урок по безопасности в сети' по ссылке 'http://kvestsetevichok.ru'.