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: интерактивная доска с ноутбуком, презентация, видео ролик, буклеты, смайлики.

Ведущий 1: Интерне́т (англ. Internet) — это всемирная система объединённых компьютерных сетей для хранения и передачи информации.
С появлением в 1969 г. Интернета весь мир поделился на два понятия:
ОНЛАЙН (Интернет) и ОФФЛАЙН (обычная, традиционная жизнь).
Практически все, что есть в ОФФЛАЙНЕ, уже присутствует и в ОНЛАЙНЕ.

В настоящее время Интернет стал неотъемлемой частью повседневной жизни, бизнеса, политики, науки и образования.

Ведущий 2: Однако бурное развитие Интернета несет также существенные издержки. Порнография, терроризм, наркотики, националистический экстремизм, маргинальные секты, неэтичная реклама и многое другое — яркие примеры контента, с которым могут соприкоснуться пользователи. В связи с этим важной проблемой, касающейся абсолютно всех, начиная от детей и заканчивая пенсионерами, является безопасность в глобальной сети.

Ведущий 1: Рассмотрим основные угрозы, подстерегающие нас во всемирной паутине.

Студент №1: Угроза № 1. Вредоносные программы (Вирусы).

Вредоносная программа – это любая программа, которая наносит вред компьютеру или пользователю этого компьютера. Некоторые виды рекламы считаются вредоносными программами.

Студент №2: Угроза № 2. Мошенничество.

Мошенничество в Интернете приобретает все большие масштабы. Изобретаются новые уловки доступа злоумышленников к компьютерам пользователей с целью выкачивания у них денег.

Ведущий 1: КАКИМ ОБРАЗОМ ЗЛОУМЫШЛЕННИКИ МОГУТ ПОЛУЧИТЬ ДОСТУП К ВАШЕМУ КОМПЬЮТЕРУ?

Первый приём. Социальная инженерия.

Это метод управления действиями человека без использования технических средств. Метод основан на использовании слабостей человеческого фактора и считается очень разрушительным.
Сегодня социальную инженерию зачастую используют в интернете для получения закрытой информации, или информации, которая представляет большую ценность. Благодаря использованию уловок и психологических приемов, вы открываете присланное хакерами письмо, содержащее вирус.

Ведущий 2: Второй приём. Фишинг («рыбалка»).

В интернете создаются подделки популярных сайтов и пользователи «клюют на эту наживку». Так вместо официальной страницы своего банка вы можете оказаться на его поддельной копии со всеми вытекающими последствиями.

Ведущий 1: Третий приём. Предложение бесплатного программного обеспечения.

Это как правило уловки, содержащие в себе множество вирусов и троянов.
Троя́нская программа (также — **троя́н, троя́нец, троя́нский конь**) — это разновидность вредоносной программы, проникающая в компьютер под видом легального программного обеспечения, в отличие от *вирусов* и *червей*, которые распространяются самопроизвольно.
В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: *сбор информации и её передачу злоумышленнику, её разрушение или злонамеренное изменение, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.*

Ведущий 2: Четвёртый приём. Блокирование операционной системы.

Еще один простой вариант получить доступ к ПК пользователя и его деньгам – заблокировать операционную систему и потребовать некоторые сведения и некоторую сумму за ее разблокировку.

Студент №3: Угроза № 3 . Интернет-зависимость.

Детская и подростковая интернет-зависимость с каждым днем набирает все большие масштабы. Общение в социальных сетях заменяют общение с родителями и сверстниками, подвижные игры и физические занятия. Теряются коммуникационные навыки. Живые эмоции заменяются «веселыми смайликами».

Углубившись в виртуальное общение, человек перестает гулять на улице, встречаться с друзьями и мало двигается, как следствие, наступают проблемы со зрением, пищеварением, опорно-двигательным аппаратом, появляется повышенная утомляемость и головокружения.

Студент №4: Угроза № 4. Пренебрежение к учебе.

В Интернет много учебного материала, который становится доступным для студентов после процедуры скачивания, занимающей не более пяти минут. Подростки распечатывают нужный реферат и сдают его преподавателю, даже не удосужившись его прочитать. Таким образом, никакие знания получены не будут. Не в помощь студенту и «решебники» по любым дисциплинам. Студент, привыкший регулярно списывать, самостоятельно перестает учить, а значит усваивать материал и развиваться.

Видеоролик!

Студент №5: Угроза № 5. Доступ к сайтам, содержащим опасную информацию.

Путешествуя по просторам Интернета легко можно оказаться на сайтах, содержащих опасную для подростков информацию. Например: *порнография, суициды, сцены насилия и жестокости, призывы к экстремистским действиям и прочее.*

Студент №6: Угроза № 6. Виртуальное общение.

Виртуальное общение - это мир фантазий. Собеседник в Интернете может выдавать себя за кого-то другого. Здесь почти у каждого есть своя маска, свой тип поведения, причем он отличается часто от реальности. Почти каждый скрыт под аватарками, вымышленными именами и своими фантазиями.

Студент №7: Угроза № 7. Интернет-хулиганство.

Одна из проблем, с которой можно столкнуться в социальных сетях - это оскорбления - *троллинг.*

Иногда это выглядит как обычное развлечение, своеобразная переписка, но очень часто *тролль* (так называют таких людей) выходит за рамки дозволенного и давит на самые болевые точки. Очень часто молодые люди, которые имеют влияние на определенную аудиторию, начинают терроризировать человека через интернет. Порой это приводит к необратимым последствиям.

Видеоролик! Фиксики!

Ведущий 1: Итак, как противостоять всем этим угрозам?

Программист: КАК ОБЕСПЕЧИТЬ ЗАЩИТУ ПК

Пользователь, который только что приобрел персональный компьютер, прежде чем начать покорять Интернет-просторы, должен:

- установить антивирус и антишпионское программное обеспечение. После установки обновить их и настроить автоматическое обновление. Лучше если обновление антивируса запускается автоматически вместе с операционной системой.
- проверять антивирусом любую устанавливаемую на ПК программу.
- Не открывать файлы, скачанные из непроверенных источников.
- Сразу удалять письма подозрительного содержания.
- Не обращать внимания на предложения легкого заработка, и уж тем более, не высылать никому своих логинов и паролей.
- При регистрации использовать сложные пароли из символов, букв и цифр. Назначайте каждый раз новый оригинальный пароль.
- Соблюдать осторожность, используя интернет в местах общего пользования.
- С платежными системами безопаснее работать через специальные приложения, а не через официальный сайт.
- Следить за интернет-трафиком. Резкое увеличение трафика безо всякой причины – серьезный повод для беспокойства.
- Игнорировать сообщения о крупных выигрышах или получении наследства.
- Использовать лицензионное ПО.
- Использовать только проверенные варианты при совершении покупок в интернет – магазинах.

Кто??: ПРАВИЛА БЕЗОПАСНОГО ПОВЕДЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ

- Не заполняйте все поля вашего профиля.
- Не нужно выкладывать в социальных сетях откровенные фотографии.
- Не регистрируйтесь под чужими данными. Если хотите сохранить инкогнито – прибегните к вымышленному имени.
- Не используйте чужие изображения без разрешения этих людей.
- Никогда не используйте социальную сеть или иной подобный сервис в качестве основного хранилища информации
- Используйте надёжный пароль. Его нужно правильно создавать, аккуратно хранить и регулярно менять.

- Выясните, какие программные способы предлагает владелец сети для защиты данных.
- Не забывайте очищать историю и удалять сохраненный пароль после работы со своим аккаунтом с чужого компьютера.
- Не участвуйте в сомнительных акциях.
- НИКОГДА не переходите по длинным ссылкам, это чаще всего путь к зараженному вирусом файлу.
- Соблюдайте культуру общения в сети.
- Не пишите в ленте о своих сомнительных с точки зрения закона «подвигах».
- Не добавляйте в друзья всех подряд.
- Не вступайте в сомнительные сообщества, куда вас приглашают непонятные люди.

Судья: ОТВЕТСТВЕННОСТЬ ЗА ИНФОРМАЦИОННЫЕ ПРАВОНАРУШЕНИЯ

Виды ответственности:

- Административная
- Уголовная
- Дисциплинарная
- Гражданско-правовая

Ответственность за экстремистские действия в сети

- Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма
  От штрафа в размере до 500 тысяч рублей до лишения свободы на срок от 2 до 5 лет.
- Распространение личной или семейной тайны человека
  От возмещения морального ущерба до лишения свободы на срок до 2 лет.
- Реабилитация нацизма
  От штрафа до 300 тысяч рублей до лишения свободы на срок до 3 лет.
- Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности России
  От штрафа в размере от 100 до 300 тысяч рублей до лишения свободы на срок до 5 лет

Ведущий2: Количество случаев привлечения к уголовной ответственности пользователей социальных сетей в России за последние годы увеличилось более чем вдвое.
Большинство подобных дел связаны со статьями Уголовного кодекса РФ, устанавливающими ответственность
за экстремизм, оскорбление и клевету.

Судья: гл. 28 «Преступления в сфере компьютерной информации» Уголовного Кодекса РФ

Статья 272. Неправомерный доступ к компьютерной информации

Т.е. информации в ЭВМ, системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ или их сети, то предусматривается наказание

- от штрафа в размере до 200 000 до лишения свободы на срок до 2 лет.

То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, - наказывается:

- штрафом в размере от 100 000 до 300 000 р. либо лишением свободы на срок до 5 лет.
  или штраф в размере зар. платы или иного дохода осужденного за период от 1 года до 2-х лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ наказываются:

- лишением свободы на срок до 3-х лет со штрафом в размере до 200 000 р.;
- Те же деяния, повлекшие по неосторожности тяжкие последствия, наказываются лишением свободы на срок от 3 до 7 лет.

Врач: ПРОФИЛАКТИКА ИНТЕРНЕТ-ЗАВИСИМОСТИ

- Сократить время, которое вы проводите в Интернете.
- Вести активный, здоровый образ жизни, распределяя время для спорта, учёбы и развлечений.
- Расширить круг общения со сверстниками.
- Поддерживать доброжелательные отношения с родителями и друзьями.

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'.

ПАМЯТКА

Быстрый поиск информации.

Как не сбиться нам с пути? Где и что в сети найти? Нам поможет непременно поисковая система. Ей задай любой вопрос, Все, что интересно. Вмиг ответ она найдет И покажет честно.

А вы знаете с кем общается ваш ребенок?

Поговорите с детьми о безопасности в Интернете

Если перейдешь меру, то самое приятное станет самым неприятным…

Демокрит

МБОУ «Удачненская школа»

Безопасный Интернет для детей.

Должны общаться дети в безопасном интернете.

Краткие правила:

Чтобы не попасть в беду - Антивирус заведу!

Злые люди в Интернете расставляют свои сети. С незнакомыми людьми ты на встречи не ходи!

В Интернете, как и в мире, есть и добрые ,и злые!

С грубиянами в сети разговор не заводи. Но и сам не оплошай -никого не обижай!

Как и всюду на планете есть опасность в Интернете. Мы опасность исключаем. если фильтры подключаем!

Если что-то не понятно, страшно или неприятно, сразу к взрослым поспеши, расскажи и покажи.

Если кто-то НЕЗНАКОМЫЙ вас попросит рассказать информацию о школе, о друзьях и телефоне, иль к страничке доступ дать. Мы на это Нет ответим, будем все держать в секрете!

Мошенничество.

Иногда тебе в сети
Могут встретиться вруны
Обещают все на свете:
Подарить бесплатно детям
Телефон, щенка, айпод
И поездку на курорт.
Их условия не сложны:
СМС отправить можно
С телефона папы, мамы-
И уже ты на Багамах.
Ты мошенникам не верь,
Информацию проверь!

Фишинг – вид интернет-мошенничества, цель которого – получить идентифицированные данные пользователей

Самый главный совет для родителей—будьте в курсе деятельности ребенка

Памятка для родителей

Второе важное правило – станьте проводником ребенка в Интернет.

Научите вашего ребенка уважению и этикету в Интернете.

Всегда помните старую поговорку «предупрежден – значит вооружен».