Классный час

Тема: «Безопасный интернет»

Цель: обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационной телекоммуникационной среде; расширение знаний о киберугрозах, формирование навыков их распознавания и оценки рисков

Задачи:

- изучение информированность пользователей о безопасной работе в сети Интернет;
- знакомство с правилами безопасной работы в сети Интернет;
- ориентироваться в информационном пространстве; способствовать ответственному использованию online-технологий;
- формирование информационной культуры обучающихся, умения самостоятельно находить нужную информацию, пользуясь web-ресурсами;
- воспитание дисциплинированности при работе в сети. Ход урока

1. Орг.момент.

- Развитие глобальной сети изменило наш привычный образ жизни, расширило границы наших знаний и опыта. Теперь появилась возможность доступа практически к любой информации, хранящейся на миллионах компьютерах во всём мире. Но с другой стороны, миллионы компьютеров получи доступ к вашему компьютеру. И не сомневайтесь, они воспользуются этой возможностью. И ни когда-то, а прямо сейчас.
- Что вы знаете об угрозах, которые исходят из Интернета?
- Перечислите опасности, которые могут угрожать человеку, его персональному компьютеру, мобильным устройствам. (На доске фиксируются ответы учеников)
- Как не стать жертвой сети Интернет? Тема нашего классного часа - «Безопасный Интернет».
- Сегодня мы ответим на 2 вопроса:

Вопрос 1. «Какие опасности подстерегают нас в Интернете?»

Вопрос 2 - главный вопрос урока: «Как сделать работу в сети безопасной?»

2. Изучение нового материала.

-Перед вами лежат листы «Рабочий лист учащегося». Сейчас мы с вами заполним его и будем продолжать заполнять в течении всего занятия. (см. Приложение 1)

- Раньше подготовка к школе заключалась в укладывании в портфель карандашей, тетрадей и учебников. Сегодня в начале этого списка нередко находится компьютер. И начать наш классный час я хочу с обработанных данных проводимого опроса. Давайте обратим внимание, что наибольший процент ответов на последний вопрос связан с безопасностью в Интернете. И ваши родители во многом правы! Очень большое внимание при работе с Интернетом необходимо уделять именно вопросам безопасности. И ответить на вопросы: «Какие опасности подстерегают нас в Интернете?» и «Как их избежать?» нам поможет этот классный час.

Вопрос 1. «Какие опасности подстерегают нас в Интернете?»

1) ***Преступники в Интернете.***

ДЕЙСТВИЯ, КОТОРЫЕ ПРЕДПРИНИМАЮТ ПРЕСТУПНИКИ В ИНТЕРНЕТЕ.

Преступники преимущественно устанавливают контакты с детьми в чатах, при обмене мгновенными сообщениями, по электронной почте или на форумах. Для решения своих проблем многие подростки обращаются за поддержкой. Злоумышленники часто сами там обитают; они стараются привлечь подростка своим вниманием, заботливостью, добротой и даже подарками, нередко затрачивая на эти усилия значительное время, деньги и энергию. Обычно они хорошо осведомлены о музыкальных новинках и современных увлечениях детей. Они выслушивают проблемы подростков и сочувствуют им. Но постепенно злоумышленники вносят в свои беседы оттенок сексуальности или демонстрируют материалы откровенно эротического содержания, пытаясь ослабить моральные запреты, сдерживающие молодых людей. Некоторые преступники могут действовать быстрее других и сразу же заводить сексуальные беседы. Преступники могут также оценивать возможность встречи с детьми в реальной жизни.

2) **<u>Вредоносные программы.</u>**

К вредоносным программам относятся вирусы, черви и «троянские кони» – это компьютерные программы, которые могут нанести вред вашему компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом и даже использовать ваш компьютер для распространения своих копий на компьютеры ваших друзей, родственников, коллег и по всей остальной глобальной Сети.

3) Интернет-мошенничество и хищение данных с кредитной карты.

В ЧЕМ СОСТОИТ МОШЕННИЧЕСТВО? Среди Интернет-мошенничеств широкое распространение получила применяемая хакерами техника «phishing»,состоящая в том, что в фальшивое электронное письмо включается ссылка, ведущая на популярный узел, но в действительности она приводит пользователя на мошеннический узел, который выглядит точно так же, как официальный. Убедив пользователя в том, что он находится на официальном узле, хакеры пытаются склонить его к вводу паролей, номеров кредитных карт и другой секретной информации, которая потом может и будет использована с ущербом для пользователя.

4) Азартные игры.

Разница между игровыми сайтами и сайтами с азартными играми состоит в том, что на игровых сайтах обычно содержатся настольные и словесные игры, аркады и головоломки с системой начисления очков. Здесь не тратятся деньги: ни настоящие, ни игровые. В отличие от игровых сайтов, сайты с азартными играми могут допускать, что люди выигрывают или проигрывают игровые деньги. Сайты с играми на деньги обычно содержат игры, связанные с выигрышем или проигрышем настоящих денег.

5) Онлайновое пиратство.

Онлайновое пиратство – это незаконное копирование и распространение (как для деловых, так и для личных целей) материалов, защищенных авторским правом – например, музыки, фильмов, игр или программ – без разрешения правообладателя.

6) Интернет-дневники.

Увлечение веб-журналами (или, иначе говоря, блогами) распространяется со скоростью пожара, особенно среди подростков, которые порой ведут интернет-дневники без ведома взрослых. Последние исследования показывают, что сегодня примерно половина всех веб-журналов принадлежат подросткам. При этом двое из трех раскрывают свой возраст; трое из пяти публикуют сведения о месте проживания и контактную информацию, а каждый пятый сообщает свое полное имя. Не секрет, что подробное раскрытие личных данных потенциально опасно.

7) Интернет-хулиганство.

Так же, как и в обычной жизни, в Интернете появились свои хулиганы, которые осложняют жизнь другим пользователям Интернета. По сути, они те же дворовые хулиганы, которые получают удовольствие, хамя и грубя окружающим.

8) Недостоверная информация.

Интернет предлагает колоссальное количество возможностей для обучения, но есть и большая доля информации, которую никак нельзя назвать ни полезной, ни надежной. Пользователи Сети должны мыслить критически, чтобы оценить точность материалов; поскольку абсолютно любой может опубликовать информацию в Интернете.

9) Материалы нежелательного содержания.

К материалам нежелательного содержания относятся: материалы порнографического, ненавистнического содержания, материалы суицидальной направленности, сектантские материалы, материалы с ненормативной лексикой.

- Послушайте данные «Лаборатории Касперского» За последний год 91% компаний, представители которых приняли участие в опросе, сталкивались с угрозами информационной безопасности. В России этот показатель еще выше – 96%. Более того, ситуация становится только хуже: почти половина участников исследования утверждает, что количество кибератак за этот период увеличилось.

- Таким образом, можно выделить 3 группы серьезных киберугроз:

1. Шпионское ПО и др. вредоносные программы,
2. Спамы,
3. Фишинговые атаки.

- Откуда может исходить опасность? (ответы детей)

- На первом месте в этом списке стоят социальные сети. Хотя в последнее время стали распространенными атаки на компьютер через мобильные устройства памяти (флешки).

Доклад учащегося

- Сегодня большинство вредоносных программ создаются либо для того, чтобы рассылать спам, либо для того, чтобы красть у пользователя важные данные. Если данные действительно важные и дорогостоящие, то для их похищения злоумышленники специально разрабатывают троян, который гарантированно будет работать на компьютерах в той организации, откуда нужно украсть данные. Осуществить внедрение такого вредоносного ПО обычно гораздо проще не через интернет, а с помощью записанных на флэшках «троянов».

Флэшки могут подбрасываться как в здание, где располагается организация, так и размещаться, скажем, на парковке рядом с ним, где их с большой долей вероятности наверняка найдёт именно сотрудник нужной организации. Поэтому если вы нашли на улице или в здании флэшку, не торопитесь радостно вставлять её в свой компьютер – лучше сначала отдайте системному администратору, который просканирует её и при необходимости обезвредит.

Игра «За или против».

- На слайде - несколько высказываний. Попробуйте привести аргументы, отражающие противоположную точку зрения.

1. Интернет имеет неограниченные возможности дистанционного образования. И это хорошо!
2. Интернет - это глобальный рекламный ресурс. И это хорошо!
3. Общение в Интернете - это плохо, потому что очень часто подменяет реальное общение виртуальному.
4. Интернет является мощным антидепрессантом.
5. В Интернете можно узнать сведения о человеке (место проживания и адрес электронной почты, номер мобильного телефона). И это хорошо!

Виртуальные грабли

Ответьте на вопросы:

- «Какие опасности подстерегают нас?»
- «Какие виртуальные грабли лежат у нас на пути?».

(Несколько учащихся подготовили короткие сообщения по темам «Интернет-зависимость», «Вредоносные и нежелательные программы», «Психологическое воздействие на человека через Интернет», «Материалы нежелательного содержания», «Интернет-мошенники»).

Физ. минутка «Собери рукопожатия».

Участникам предлагается в течение 10 секунд пожать руки как можно большего числа других людей. Обсуждение.

- Кому сколько человек удалось поприветствовать? У кого-то возник психологический дискомфорт? Если - да, то чем он был вызван? Анализ ситуации.
- Общаясь в Интернете, мы очень часто добавляем незнакомых людей в свои социальные сети и общаемся с ними. Мы не знаем про них ничего, только их Ники. Как много информации про человека мы можем узнать от Ника или рукопожатия? Однако, очень важно знать, что есть рядом люди, готовые выслушать, оказать поддержку, помочь в трудную минуту

-Давай те ответим на главный вопрос урока - «Как сделать работу в сети безопасной?»

3. Практическая работа.

-Сформулируйте правила безопасной работы в сети Интернет.

Резюме (обсуждение найденной информации). Какие правила безопасной работы выбрали обучающиеся, посещая web-сайты?

- Дайте определения основным угрозам в сети Интернет. Составьте правила безопасного поведения в сети Интернет.

4. Закрепление изученного материала.

Вопрос2. «Как этих опасностей избежать?»

1) **Преступники в Интернете.**

Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие сексуальные намеки. Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете.

2) **Вредоносные программы.**

А) Никогда не открывайте никаких вложений, поступивших с электронным письмом, за исключением тех случаев, когда вы ожидаете получение вложения и точно знаете содержимое такого файла.

Б) Скачивайте файлы из надежных источников и обязательно читайте предупреждения об опасности, лицензионные соглашения и положения о конфиденциальности.

В) Регулярно устанавливайте на компьютере последние обновления безопасности и антивирусные средства.

3) **Интернет-мошенничество и хищение данных с кредитной карты.**

А)Посещая веб-сайты, нужно самостоятельно набирать в обозревателе адрес веб-сайта или пользоваться ссылкой из «Избранного» (Favorites); никогда не нужно щелкать на ссылку, содержащуюся в подозрительном электронном письме.

Б) Контролируйте списание средств с ваших кредитных или лицевых счетов. Для этого можно использовать, например, услугу информирования об операциях со счетов по SMS, которые предоставляют многие банки в России.

4) Азартные игры.

Помните, что нельзя играть на деньги. Ведь, в основном, подобные развлечения используются создателями для получения прибыли. Игроки больше теряют деньги, нежели выигрывают. Играйте в не менее увлекательные игры, те, которые не предполагают использование наличных или безналичных проигрышей/выигрышей.

5) Онлайновое пиратство.

Помните! Пиратство, по сути, обычное воровство, и вы, скорее всего, вряд ли захотите стать вором. Знайте, что подлинные (лицензионные) продукты всегда выгоднее и надежнее пиратской продукции. Официальный производитель несет ответственность за то, что он вам продает, он дорожит своей репутацией, чего нельзя сказать о компаниях – распространителях пиратских продуктов, которые преследуют только одну цель – обогатиться и за счет потребителя, и за счет производителя. Лицензионный пользователь программного обеспечения всегда может рассчитывать на консультационную и другую сервисную поддержку производителя, о чем пользователь пиратской копии может даже не вспоминать. Кроме того, приобретая лицензионный продукт, потребитель поддерживает развитие этого продукта, выход новых, более совершенных и удобных версий. Ведь в развитие продукта свой доход инвестирует только официальный производитель.

6) Интернет-дневники.

Никогда не публикуйте в них какую-либо личную информацию, в том числе фамилию, контактную информацию, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения. Никогда не помещайте в журнале провокационные фотографии, свои или чьи-либо еще, и всегда проверяйте, не раскрывают ли изображения или даже задний план фотографий какую-либо личную информацию.

7) Интернет-хулиганство.

Игнорируйте таких хулиганов. Если вы не будете реагировать на их воздействия, большинству гриферов это, в конце концов, надоест и они уйдут.

8) Недостоверная информация.

Всегда проверяйте собранную в Сети информацию по другим источникам. Для проверки материалов обратитесь к другим сайтам или СМИ – газетам, журналам и книгам.

9) Материалы нежелательного содержания.

Используйте средства фильтрации нежелательного материала (например, MSN Premium’s Parental Controls или встроенные в Internet Explorer®). Научитесь критически относиться к содержанию онлайновых материалов и не доверять им.

- Перед вами лежат листы с тестами. Ответьте на вопросы теста. (см. Приложение 2)

Интернет - это новая среда взаимодействия людей. В ней новое звучание приобретают многие правила и закономерности, известные людям с давних времен. Попробую сформулировать некоторые простые рекомендации, используя хорошо известные образы.

- Какой можно сделать вывод по теме нашего урока? (ответы детей)

Рефлексия. На данном этапе предлагается подвести итоги урока Интернет- безопасности: на столе лежат три смайлика, обучающимся необходимо выбрать и обвести тот, который соответствует настроению школьника (см. Приложение 3)

- Урок понравился. Узнал что-то новое.
- Урок понравился. Ничего нового не узнал.
- ***Урок не понравился. Зря время потерял.***

И помните, Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но - как и реальный мир - Сеть тоже может быть опасна!