

Беседа «Безопасный Интернет»

5класс

Цель урока: развить информационную компетентность учащихся, обучить правилам безопасной работы в Интернете.

Задачи урока:

- обучающие: познакомить с опасными и безопасными сторонами Интернета; сформировать у учащихся понятия о существующих угрозах Интернета и способах их избежать; обобщить с учащимися материал по теме «Безопасный Интернет».

-развивающие : развивать внимание, память, умение обобщать знакомый материал по теме, развивать познавательные навыки.

-воспитательные :воспитание информационной культуры учащихся, безопасности.

Формы работы учащихся: индивидуальная, групповая.

Оборудование: компьютер, мультимедийный экран, доска, мел.

Раздаточный материал: листы формата А4, цветные карандаши.

Методические приемы: беседа, монолог, групповая работа, анализ, подведение итогов.

Ход классного часа:

Классный руководитель: Добрый день, дорогие ребята. Темой нашего сегодняшнего классного часа будет...(учитель делает паузу).Посмотрите, пожалуйста на экран, прочитайте высказывание.

Ученик: Виртуальная сказка с виртуальным концом

Все волшебно и ярко, но с закрытым лицом

Ничего не понятно , где тут правда и ложь

И пытаться не надо, все равно не поймешь

Классный руководитель: Как вы думаете, о чем же мы сегодня поговорим с вами?

Ученик: Я думаю, мы будем говорить об Интернете.

Классный руководитель: Абсолютно верно, тема нашего класса «Безопасный Интернет».

Вы знаете, что сеть Интернет называют Всемирной паутиной, давайте мы с вами нарисует подобную паутину, в которой обозначим ответы на вопрос «Зачем нам нужен Интернет?»

Учащийся рисует на доске кластер в центре которого помещает слово «Интернет».



Ученик1- Чтобы получать новую информацию.

Ученик 2- Для того, чтобы общаться с друзьями.

Ученик 3- Мне интернет помогает больше узнавать об интересующих меня событиях и помогает получать больше информации для подготовки к урокам в школе.

Ученик 4 –В сети Интернет я посещаю образовательные сайты и они помогают мне подготовиться к предстоящим ОГЭ.

Ученик 5- Я люблю смотреть фильмы в сети Интернет.

Ученик 6- А я играю в интернет-игры с свободное время.

Классный руководитель – Спасибо вам за ответы, у нас получилась паутина, в которую каждый из нас попадает и для многих эта паутина становится очень опасной. Как вы думаете, какую опасность хранит в себе Интернет?

Ученик1- Существует угроза заражения вредоносным ПО.

Классный руководитель- Кто может рассказать подробнее об этой опасности?

Ученик1-Компьютер может быть заражен вредоносными программами, которые могут нанести вред компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом и даже использовать компьютер для распространения своих копий на компьютеры по всей остальной глобальной сети.

Классный руководитель- Спасибо, ты прав, для того, чтобы избежать такой ситуации вам необходимо не запускать файлы, присланные вам по почте, ICQ и т.д. без предварительной проверки на вирусы (и даже после этого, файлы, от сомнительных людей лучше подвергнуть тщательной проверке, например с помощью антивируса с последним обновлением).

Ученик 2- Я могу привести пример. "Хакер" прикидывается человеком противоположного пола и вступает с жертвой в разговор, заинтересовав разговором, он под каким - либо предлогом устроит обмен фотографиями, только жертва ему пошлет нормальную фотографию, а "хакер" пошлет обыкновенный «троян» со стандартной иконкой от jpg файлов. Как только жертва подаст команду, троян выполнит свое черное дело, заразив систему и распаковав из своего тела небольшую фотографию. Жертва скорее всего не сразу догадается, о том что произошло, ну а последствия могут быть очень серьезными.

Классный руководитель- Спасибо, очень полезное предупреждение.

Ученик1- Я могу привести в пример еще 1 вид угрозы. Интернет-мошенничество. Самое широкое распространение получила применяемая хакерами техника «фишинг», 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.

Ученик 2- Я лично столкнулся с таким видом мошенничества. Когда, якобы моя сестра, написала мне в социальной сети письмо с просьбой отправить со своего номера телефона код на вход на сайт. На который она войти не может, как только я это сделал, баланс моего телефона сократился на 400 рублей, а потом выяснилось, что страничка сестры была взломана и ею воспользовались мошенники

Классный руководитель- Какой вывод мы можем сделать?

Ученик 3-Нельзя отправлять свои данные на неизвестный вам номер, необходимо убедиться, что в вашей помощи нуждаются ваши родственники или знакомые.

Классный руководитель- Я знаю, что многие из вас общаются в социальных сетях. Так ли это безопасно?

Ученик 1-Я думаю, что есть опасность и в общении в социальных сетях.

Например, все мы публикуем там настоящие имя, фамилию, дату рождения, интересы и увлечения, а ведь этой информацией могут воспользоваться мошенники и хулиганы.

Ученик 2- Мы выкладываем свои фотографии, глядя на которые можно увидеть обстановку нашей квартиры и понять достаток семьи, а этой информацией могут воспользоваться воры, тем более, как уже было сказано, у них есть наша личная информация.

Ученик 3- В социальных сетях каждый человек может выдать за себя за другого, порой, такое общение опасно, кто знает, что в голове у того, кто ведет с нами переписку.

Классный руководитель- Как много опасности и в социальных сетях. Как же нам ее избежать?

Ученик 1- Не выкладывать точную и полную информацию о себе.

Ученик 2- Не выкладывать фотографии, сделанные в квартире.

Учитель 3- Общаться только со знакомыми нам или нашим друзьям.

Классный руководитель- Молодцы, делаете правильные выводы. Хотелось бы добавить, что злоумышленники могут использовать различные методы социальной инженерии (угрозы, шантаж, игру на чувствах жертвы — например, жадности или сочувствии), чтобы выманить деньги. В таких случаях они пишут письма определенного сценария. Один из примеров — так называемые «нигерийские письма», в которых автор обещает жертве огромную прибыль взамен на небольшие накладные расходы.

Пример «нигерийского письма»:

«Дорогой друг!

Я миссис Сесе-секо, вдова бывшего президента Заира (ныне Демократической республики Конго) Мобуту Сесе-секо. Я вынуждена написать Вам это письмо. Это в связи с моими нынешними обстоятельствами и ситуацией. Я спаслась вместе со своим мужем и двумя сыновьями Альфредом и Башером в Абиджан, Кот-д'Ивуар, где мы и поселились - затем мы переехали в Марокко, где мой муж умер от рака. У меня есть банковский счет на сумму 18 000 000 (восемнадцать миллионов) долларов США. Мне нужно ваше желание помочь нам - чтобы вы получили эти деньги для нас, в

таком случае я представлю Вас моему сыну Альфреду, который имеет право получить эти деньги. Я хочу инвестировать эти деньги, но не хочу, чтобы было известно, что это делаю я. Мне хочется приобрести недвижимость и акции транснациональных компаний, а также вложиться в надежные и неспекулятивные дела, которые Вы посоветуете. При получении подобных писем необходимо внимательно изучить информацию из него. Проверить достоверность описанных фактов. Если в письме предлагается большая выгода за незначительное вознаграждение, скорее всего, оно мошенническое. Игнорировать такие письма.

Также существует выманивание SMS-пароля незнакомцем. Пользователю может прийти SMS от банка или платежного сервиса с паролем для совершения платежа. Сразу после этого может позвонить человек, который скажет, что ввел этот номер мобильного телефона по ошибке и попросит сообщить код из SMS, которое только что пришло пользователю. На самом деле код из SMS — это пароль не к счету незнакомца, а к счету пользователя, с помощью которого злоумышленник может поменять настройки кошелька или интернет-банка, украсть деньги и т.д. Поэтому нельзя никому сообщать пароли, пин-коды и коды из SMS, которые приходят на мобильный номер от банков, платежных сервисов, а также мобильных операторов.

Классный руководитель- Девушки нашего класса любят посещать интернет сайты магазинов, всегда ли это безопасно?

Ученик1-Нет, так как многие онлайн магазины могут быть «фэйками», от слова «подделка», такие сайты получают деньги от покупателей, но не присылают обещанного товара, а закрывают свои странички. Адреса таких сайтов могут совпадать с оригинальными сайтами, отличаясь лишь 1 буквой.

Классный руководитель-Поэтому необходимо не доверять объявлениям о подозрительно дешевых товарах. Перед покупкой искать отзывы в интернете об интернет-магазине или частном продавце, который предлагает товар. Если информации нет или ее недостаточно, отказаться от покупки.

Ученик 1- Вот, поэтому я не смотрю сайты магазинов, а смотрю фильмы и видео онлайн, это-безопасно!

Классный руководитель- Ты знаешь, ты не совсем прав. Часто, чтобы скачать бесплатный файл или посмотреть видео в хорошем качестве без рекламы, сайты предлагают ввести мобильный номер. Если сделать это, включится подписка и с указанного номера могут начать списываться деньги. Поэтому ты должен не указывать свой мобильный номер на незнакомых сайтах, а если подписка уже оформлена, позвонить в службу поддержки оператора и попросить отключить её. В этом случае, просмотр фильмов-безопасен и остается помнить лишь о возрастных ограничениях в просмотрах фильмов.

Классный руководитель- Вы знаете, что существует ст. 5 Федерального Закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», однако, существует угроза кибербуллинга. Кто может нам сказать, что обозначает это слово?

Ученик 1- Я думаю, что «кибер» -это от слова англ.языка «cyber»,а «булинг» от «bullying»-хулиганство.

Классный руководитель- Ты абсолютно прав. Кибербулинг-преследование сообщениями, содержащими оскорбления, агрессию, запугивание, хулиганство, социальное бойкотирование с помощью различных интернет-сервисов. Поэтому при общении в Интернете вы должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов – читать грубости также неприятно, как и слышать и правильно реагировать на обидные слова или действия других пользователей. Нельзя использовать Сеть для хулиганства, распространения сплетен или угроз. Предлагаю вам записать адрес сайта «Дети онлайн» www.detionline.com , где открыта линия телефонного и онлайн-консультирования, которая оказывает психологическую и информационную поддержку детям и подросткам, столкнувшимся с различными проблемами в Интернете. Обратиться на Линию помощи можно и по телефону 8-800-25-000-15, бесплатно позвонив из любой точки страны, либо по электронной почте: helpline@detionline.com. Звонки принимаются в рабочие дни с 9.00 до 18.00.

Предлагаю вам объединиться в группы по 6 человек и сделать листовки о безопасном поведении в сети Интернет. (Учитель раздает учащимся листы А3 и цветные карандаши). На выполнение задания отводится 5 минут.

Прочитайте содержимое своих листовок всему классу, пожалуйста.

(Учащиеся выходят к доске и зачитывают листовки).

Классный руководитель- Спасибо, у вас получились замечательные работы. Предлагаю разместить их в уголке класса, чтобы с ними могли ознакомиться учащиеся нашей школы.

К сожалению, наш классный час подошел к концу, надеюсь, вы узнали сегодня много полезной информации и знаете как надо себя вести, чтобы не попасться в сети Сети.

На партах у вас лежат листочки с анкетой, прошу вас заполнить ее.

1. Выберите правильные ответы на вопрос "Чем полезен Интернет?":

- a. на множестве сайтов можно найти массу полезной информации
- b. воздействием на неокрепшую психику и ум ребенка
- c. возможностью общаться по электронной почте
- d. неограниченным доступам к нежелательному содержимому
- e. возможностью совершать путешествия, посещать выставки и музей, не выходя из дома

2. Выберите правильные ответы на вопрос "Чем опасен Интернет?":

- a. возможностью возникновения Интернет-зависимости
- b. потенциальным доступом к Вашим личным данным
- c. возможностью заражения вредоносным ПО
- d. контактами с незнакомыми людьми с помощью чатов или электронной почты
- e. возможностью заказать необходимые вещи не выходя из дома

3. Какой термин описан ниже?

"Навязчивое желание подключиться к Интернету и болезненная неспособность вовремя отключиться от него".

Ответ: Интернет-зависимость.

4. Как преодолеть Интернет-зависимость?

- a. вести здоровый образ жизни
- b. переключиться на игры в телефоне
- c. общаться с живой природой
- d. заниматься творчеством
- e. больше смотреть телевизор

5. Какое понятие описано ниже?

«Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам и паролям».

Ответ: фишинг.

6. Выберите ответ на вопрос "Как обезопасить себя на Интернет-аукционах?"

- a. не сообщать номера своих кредитных карт
- b. не доверять слишком привлекательным предложениям
- c. перед покупкой получить полную информацию о продавце
- d. всегда покупать товары со скидками и по различным акциям
- e. покупать товары только на проверенных сайтах

Ответ: a, b, c, e.

7. Какие сайты лишнее?

- a. образовательные сайты
- b. официальные сайты поиска работы в вашем городе
- c. сайты с рекламой табака и алкоголя
- d. сайты, посвященные морфологическим словарям и проверке правописания
- e. топографические сайты

Ответ: сайты с рекламой табака и алкоголя.

8. Как следует вести себя при работе в Интернете?

- a. говорить взрослым, если кто-то в Сети надоедает тебе
- b. посещать музеи, выставки, картинные галереи, пользуясь возможностями Сети
- c. не обмениваться с незнакомцами фотографиями через Интернет
- d. рассказывать незнакомым людям информацию о себе и своей семье
- e. не открывать электронные сообщения от незнакомых людей и не Ученики выполняют задание-рефлексию.

Классный руководитель-Спасибо вам за активное участие в классном часе.
Давайте соблюдать правила безопасного поведения в сети Интернет.

Используемая литература:

1. Сайт [http://www. supertosty.ru/](http://www.supertosty.ru/)
2. Разработка классного часа Могуновой О.С. «Интернет :как избежать опасности»
3. Сайт [http://www. sklyarinfo.ru/](http://www.sklyarinfo.ru/)
4. Сайт [http://www. apkro.ru.content.blogcategory/](http://www.apkro.ru.content.blogcategory/)