**МКОУ**

**«Ортастальская СОШ им.Р.Халикова»**



**Тема урока:** **Безопасный Интернет**

**Учителя информатики:**

Рамазанова Заира Магомедафисовна

**2019**



Урок **«Киберугрозы современности: главные правила их распознавания и предотвращения»**

*Форма занятия:* семинар

*Цель:*

расширение знаний о киберугрозах, формирование навыков их распознавания и оценки рисков.

Возраст обучающихся: 6-9 класс.

*План занятия:*

1. Обсуждение правил предотвращения киберугроз, которые встречаются при работе в Интернете. Составление листовок «Правила защиты от киберугроз»

2. Практикум «Опасность 419»

3. Подведение итогов занятия.

*Ход занятия.*

Занятие начинается показом социального видеоролика «Безопасный интернет - детям!». После просмотра ролика учитель объявляет тему занятия и предлагает ученикам самим сформулировать цель занятия.

Обсуждение правил предотвращения киберугроз, которые встречаются при работе в Интернете. Продолжительность 20 минут.

У каждого ученика на столе лежит чистый лист бумаги – заготовка листовки по безопасности в Интернете. Перед тем, как начать работать учитель объясняет, что по ходу обсуждения каждый ученик должен заполнять листовку правилами, которые ему кажутся необходимыми и важными. После того, завершения обсуждения, отдельные ученики зачитывают свои листовки, остальные могут добавлять правила. Листовки собираются после урока для того, чтобы их раздать ученикам других классов.

Учитель начинает обсуждение с вопроса к аудитории: «Что вы знаете об угрозах, которые исходят из Интернета?» Просит учеников перечислить опасности, которые могут угрожать человеку, его персональному компьютеру, мобильным устройствам. На доске фиксируются ответы учеников.

После короткого обсуждения учитель приводит 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. Перечисляя киберугрозы, которые представляются им самыми значительными, большинство участников исследования во всем мире ставят на первое место вирусы, шпионское ПО и другие вредоносные программы (61%). Спам назвали источником угрозы 56% респондентов. Третье место (36%) заняли фишинговые атаки, за ними идут сбои, вызванные проникновением в корпоративную сеть (24%), и DDoS-атаки (19%).

Таким образом, можно выделить 3 группы серьезных киберугроз:

* Шпионское ПО и др. вредоносные программы,
* Спамы,
* Фишинговые атаки.

Обсуждение основных правил защиты от главных киберугроз. Все ответы детей записываются на доске.

При обсуждении внимание учеников обращается на то, откуда могут исходить опасность. На первом месте в этом списке стоят социальные сети. Хотя в последнее время стал распространенными атаки на компьютер через мобильные устройства памяти (флешки).

*«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.*

*Бывают и более банальные, но не менее эффективные способы заразить компьютер недостаточно осторожного пользователя. Например, от знакомого по Skype Вам может прийти сообщение в духе «Посмотри, на этой фотографии он так похож на нашего друга (одноклассника)!», ну и, конечно, ссылка на саму эту фотографию. При переходе по ссылке фотография почему-то не открывается в браузере, а сохраняется на жесткий диск, но мало кто на это обращает внимание. Хотя они-то как раз и должны насторожить! В общем, когда «фото» не открывается, пользователь «входит» в папку с ним, и видит, что это не просто abcd.jpg, а abcd.jpg.scr, то есть, исполняемый файл, а его компьютер уже заражен вирусом».* После обсуждения листовок на доске должен быть записаны основные правила защиты от киберугроз.

**Практикум «Угроза 419».**

***Цель:*** формирование навыков распознавание спама в «нигерийских письмах».

Одной из разновидностей спама являются «Нигерийские письма» или другое название «Угроза 419». «Нигерийские письма» - вид мошенничества, получивший наибольшее развитие с появлением спама. Называется так потому, что письма особое распространение получили в Нигерии, причем еще до распространения Интернета они распространялись по обычной почте, начиная с середины 1980 годов. С появлением интернета «Нигерийские письма» стали нарицательным понятием.

Как правило, у получателя письма просят помощь в многомиллионных операциях, обещая солидные проценты с сумм. Если получатель согласится, у него выманиваются всё большие суммы денег на сборы, взятки и т. д. В худших вариантах жертве предлагается полулегально прибыть в Нигерию, где его либо арестовывали за незаконное прибытие в страну и у него вымогаются деньги за освобождение, либо похищали с целью получения выкупа.

Мошенничество профессионально организовано: у мошенников есть офисы, работающий факс, часто мошенники связаны с правительственными организациями, и попытка получателя письма провести самостоятельное расследование не обнаруживает противоречий в легенде. Сделка подаётся как «безвредное» беловоротничковое преступление, что мешает жертве обратиться к властям. Разумеется, обещанных денег жертва в любом случае не получает: их просто не существует.

Спамеры оперативно реагируют на ситуацию в мире, отслеживая очаги нестабильности. Поэтому постоянно появляются новые разновидности «Нигерийских» писем — например, «кенийские» или «филиппинские». Во время войны в Ираке активно шли спамерские рассылки «иракского» спама.

Подавляющее большинство «нигерийского» спама идет на английском языке, но в 2004-2005 гг. спамеры взялись активно осваивать Рунет. Появился «нигерийский» спам на русском языке, эксплуатирующий горячие события российской политической жизни.

«Нигерийские письма» являются дидактическим инструментом для формирования навыков распознавания спама и фишинговых атак.

Учитель делит аудиторию на 4 группы. Каждой группе выдает конверт, в котором содержится образец «нигерийского письма» (Приложение) и задание:

1. Внимательно прочитайте текст письма.

2. Выделите в нем моменты, указывающие на то, что это спам.

3. Перечислите факты, указанные в письме, которые кажутся вам недостоверными, подозрительными.

После того, как группы выполнят задание, начинается коллективное обсуждение. Вопросы для обсуждения:

1. Как можно распознать «нигерийское письмо»?

2. Как вы думаете кто авторы «нигерийских писем»?

3. Какую цель преследуют авторы «нигерийских писем»?

4. Можно ли считать безвредными «нигерийские письма»?

Результаты работы группы представляет один ученик. Все остальные ученики могут задавать вопросы и высказывать свое мнение. Учитель на доске записывает главные особенности «Нигерийских писем», которые нашли ученики, дополняет, систематизирует.

Подведение итогов занятия.



**День медиабезопасности.**



**День медиабезопасности**

**Классный час «Способы защиты информации»**

Рамазанова Заира Магомедафисовна

Класс: 11

Цель: Познакомить учащихся с опасностями, которые подстерегают их в сети Интернет и способах защиты информации.

1. Ваш незащищенный компьютер — орудие преступления в руках кибермошенников

Без надежной системы защиты компьютер становится легкой добычей для киберпреступников. Ваш ПК может стать частью мошеннической зомби-сети и использоваться для проведения сетевых атак, шантажа и рассылки спама. Все это может происходить без вашего ведома и вскоре из виртуального соучастника киберпреступлений вы становитесь реальным — за участие в DDoS-атаке правоохранительные органы имеют право конфисковать ваш компьютер.

Правильные привычки:

Применяйте комплексные средства защиты (файловый/почтовый/веб-антивирус + сетевой экран) с обновленными антивирусными базами и крайне осторожно относитесь к файлам, которые получаете из сети. Перед тем как запустить файл, обязательно проверьте его на наличие вирусов.

Проводите регулярную ревизию и обновление используемого вами ПО.

Пользуйтесь только хорошо зарекомендовавшими себя источниками программ и прочих файлов.

Периодически сохраняйте на внешнем носителе файлы, с которыми ведется работа. Затраты на копирование файлов, базы данных, документацию, значительно меньше затрат на восстановление этих файлов при сбое компьютера.

Используйте только лицензионные приложения. Некоторые бесплатные, условно-бесплатные и тем более пиратские копии программ способны нанести больший ущерб компьютеру, чем сам вирус.

Ограничивайте круг лиц, допущенных к работе на вашем компьютере. Как правило, наиболее часто подвержены заражению «многопользовательские» персональные компьютеры.

Вывод: компьютер с комплексной антивирусной защитой — головная боль для киберпреступников!



2. Будьте бдительны: интернет-аферисты не дремлют!

Широкое использование приемов социальной инженерии, основанных на знании практической психологии, позволяет сетевым злоумышленникам быстро достичь своей цели. Ссылки на подложные сайты, SMS-мошенничество, онлайн-лотереи, финансовые пирамиды, фальшивые антивирусы — вот наиболее популярные виды интернет-мошенничества. Доверяя всему, что предлагается в интернете и не следуя элементарным правилам компьютерной безопасности, вы становитесь легкой добычей киберпреступников и можете понести серьезные финансовые потери.

Правильные привычки: отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат — действительно тот, за кого себя выдает задавайте больше вопросов: получив сообщение с ссылкой в ICQ/QIP или личное сообщение в социальной сети, убедитесь, что это не автоматическая рассылка с зараженного компьютера трезво относитесь к спам-предложениям: не верьте в неожиданные выигрыши, не откликайтесь на предложения бесплатных товаров или дешевых лекарственных средств используйте настоящие программы защиты: антивирус, требующий деньги за удаление вредоносной программы с компьютера, является фальшивым уточняйте настоящую стоимость SMS-сообщений на короткие номера не доверяйте сообщениям «Проголосуй за меня SMSкой в конкурсе» или «Помоги мне — у меня проблемы» проверяйте информацию об SMS-акциях на сайтах их устроителей не устанавливайте неофициальные дополнения и улучшения к играм проверяйте подлинность адреса в строке браузера при вводе персональных данных на игровом сайте отвечая на письма от имени администрации игрового сервера, удостоверьтесь, что они подлинные не доверяйте игрокам, которые предлагают прислать вам какие-либо данные от игры — подобные файлы могут содержать вредоносный код

Вывод: не спешите доверять любым предложениям в Сети.

3. «Кража личности»: защищайте свое виртуальное «я»

Использовать один простой пароль для электронной почты, ICQ или своих аккаунтов в социальных сетях — то же, что ключом от почтового ящика закрывать входную дверь. Оставляя много личной информации в сети, вы рискуете сделать свои персональные данные доступными мошенникам, которые с их помощью могут от вашего имени рассылать электронные письма, вести ICQ-общение, совершать телефонные звонки или, проникнув в ваш компьютер, уничтожить ценные данные.

Правильные привычки:

Ограничьте объем информации о себе, находящейся в публичном доступе. Заведите себе два адреса электронной почты — частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный — для публичной деятельности (форумов, чатов и так далее). Адрес для переписки не должен быть легким в запоминании или «красивым». Чем длиннее адрес и чем менее он удобочитаем — тем лучше. Используйте только сложные пароли. Для разных учетных записей и сервисов используйте разные пароли. Не передавайте свои логин и пароль третьим лицам.

Вывод: используйте сложные и разные пароли для своего компьютера!

4. Не дайте пиратам взять себя в заложники — откажитесь от использования пиратского ПО

Выбирая нелегальное программное обеспечение, вы получаете менее надежный продукт — значительное число пиратских программ содержат в себе уязвимости, эксплуатируемые киберпреступниками для получения доступа к вашему компьютеру. Отсутствие сервиса поддержки со стороны квалифицированных специалистов значительно сужает поле применения используемого вами ПО: так, без своевременного обновления антивирусных баз системы антивирусной защиты фактически неэффективны. Нередко под видом бесплатных программ в интернете распространяются вредоносные программы.

Правильные привычки: Используйте только лицензионное ПО (либо свободно распространяемое ПО из надежных источников) — гарантию стабильной работы вашего ПК и сохранности ваших данных. Следите за специальными акциями и скидками на легальную продукцию (например, некоторые компании предлагают перейти с пиратской копии продукта на легальную со значительной скидкой). В случае возникновения вопросов или трудностей в работе с используемыми программами обратитесь в службу технической поддержки — обладатели легальных копий ПО имеют такую возможность.