МБОУ «Ишхой-Юртовская СШ имени Абдулмежидова М.Д.»

Гудермесский муниципальный район ЧР.

Урок на тему:

**«Безопасность в сети Интернет»**

учитель информатики и ИКТ

Макаева Н.Х.

2018г

**Тема: Безопасность в сети «Интернет»**

**Цели:**

1) обеспечение информационной безопасности обучающихся путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

2) развивать умение анализировать и систематизировать имеющуюся информацию.

3)воспитывать навыки информационной культуры в сети Интернет.

**Задачи:**

ознакомить учащихся:

– с правилами ответственного и безопасного поведения в современной информационной среде, способах защиты от противоправных посягательств в сети Интернет;

– как критически относиться к сообщениям в СМИ (в т.ч. электронных), как отличить достоверные сведения от недостоверных, как избежать вредной и опасной для них информации, как распознать признаки злоупотребления их доверчивостью и сделать более безопасным свое общение в сети Интернет;

– как общаться в социальных сетях (сетевой этикет), не обижая своих виртуальных друзей, и избегать выкладывать в сеть компрометирующую информацию или оскорбительные комментарии и т.д.

Оборудование: компьютер, проектор, тетрадь.

Ход урока:

1. **Орг. момент.**

Добрый день. Тема нашего урока «Безопасность в сети Интернет». Интернет стал неотъемлемой частью нашей жизни. Вместе с тем интернет таит в себе опасности о них необходимо знать, чтобы избегать их.

**II. Изучение нового материала.**

**Как вы думаете, какие опасности могут поджидать нас в интернете?**

В первую очередь это действия мошенников, которые хотят получить финансовую или иную выгоду. Мошенники могут использовать самые разные инструменты и методы — например, вирусное программное обеспечение (или «вирусы»), поддельные сайты, мошеннические письма, перехват и подбор паролей к учетным записям в социальных сетях и на почтовых сервисах. Давайте поподробнее разберемся, как с этим бороться.

**А как вы понимаете, что такое «вирус»?**

Давайте запишем определение в тетрадь.

*Вирус- вредоносная программа, способная самопроизвольно внедряться и внедрять свои копии в другие программы, файлы, системные области компьютера, с целью создания всевозможных помех работе на компьютере.*

**А как вы считаете, какие рекомендации нужно соблюдать для предотвращения попадания вируса на ваш компьютер?** Давайте их запишем.

Рекомендации

• Используйте антивирусное программное обеспечение с обновленными

базами вирусных сигнатур.

• Не открывайте вложенные файлы или ссылки, полученные по электронной

почте, через социальную сеть или другие средства связи, не

удостоверившись, что файл или ссылка не содержит вирус.

• Внимательно проверяйте доменное имя сайта (например, www.yandex.ru),

так как злоумышленники часто используют похожие имена сайтов, чтобы

ввести жертву в заблуждение (например, www.yadndex.ru).

• Обращайте внимание на предупреждения браузера или поисковой машины

о том, что сайт может угрожать безопасности компьютера.

• Не подключайте к своему компьютеру непроверенные съемные носители.

• Не поддавайтесь на провокации злоумышленников, например, требование

перевести деньги или отправить смс, чтобы снять блокировку компьютера.

Злоумышленники часто стремятся получить доступ к аккаунтам жертвы,

например, в социальных сетях, на почтовых и других сервисах. Украденные

аккаунты они используют, в частности, для распространения спама и вирусов.

**Какими способами мошенники могут получить доступ к учeтной записи жертвы?**  Давайте запишем.

*Мошенники могут получить доступ к учeтной записи жертвы следующими*

*способами:*

*• Заставить жертву ввести свои данные на поддельном сайте.*

*• Подобрать пароль жертвы, если он не сложный.*

*• Восстановить пароль жертвы с помощью «секретного вопроса» или*

*указанной при регистрации электронной почты.*

*• Перехватить пароль жертвы при передаче по незащищенным каналам*

*связи.*

Как правило, для кражи личных данных используются фишинговые сайты. Фишинг(от англ. **fishing** — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Злоумышленники создают фишинговые сайты, копирующие интерфейс известных ресурсов, а жертвы вводят на них свои логины и пароли, не понимая, что сайты поддельные.

**Каким рекомендациям нужно следовать, чтобы предотвратить это?**

Давайте запишем.

*Рекомендации*

*• Используйте сложные пароли (они состоят как минимум из 10 символов,*

*включают буквы верхнего и нижнего регистра, цифры и специальные*

*символы, не содержат имя пользователя и известные факты о нем).*

*• Никому не сообщайте свой пароль.*

*• Для восстановления пароля используйте привязанный к аккаунту*

*мобильный номер, а не секретный вопрос или электронную почту.*

*• Не передавайте учетные данные — логины и пароли — по незащищенным*

*каналам связи (не защищены, как правило, открытые и общедоступные wi-fi*

*сети).*

*• Внимательно проверяйте доменные имена сайтов, на которых вводите*

*учетные данные.*

Печальная действительность современного интернета такова, что на 100% только сам пользователь сможет защитить себя от посягательств извне. Пользователь должен осознать, что ему не стоит запускать различного рода программы, присланные тем или иным "доброжелателем", не скачивать сомнительные файлы с непроверенных серверов в Сети, не идти на поводу у людей, которые, на первый взгляд внушают, доверие.

**III. Закрепление.**

**Выполнение проверочного теста.**

**Тест №1 «Осторожно, Интернет!»**

**1. Какую информацию нельзя разглашать в Интернете?**

1. Свои увлечения .

2. Свой псевдоним .

3. Домашний адрес.

**2. Чем опасны социальные сети?**

1. Личная информация может быть использована кем угодно в разных целях .

2. При просмотре неопознанных ссылок компьютер может быть взломан .

3. Все вышеперечисленное верно .

**3. Виртуальный собеседник предлагает встретиться, как следует поступить?**

**1.** Посоветоваться с родителями и ничего не предпринимать без их согласия .

**2.** Пойти на встречу одному .

**3.** Пригласить с собой друга .

**4. Что в Интернете запрещено законом?**

1. Размещать информацию о себе.

2. Размещать информацию других без их согласия .

3. Копировать файлы для личного использования .

**5. Действуют ли правила этикета в Интернете?**

1. Интернет - пространство свободное от правил .

2. В особых случаях .

3. Да, как и в реальной жизни.

**VI. Практическая работа.**

**Работа в группах.** Составление правил безопасного использования сети интернет.

1. 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.
2. Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть ваш разговор, т.к. он может быть записан.
3. 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 посылаясь вам спам.
4. Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.
5. Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя в вашем отношении неподобающим образом, сообщите об этом.
6. Если вас кто-то расстроил или обидел, расскажите все взрослому.

**V. Рефлексия. Подведение итогов работы.**

Учащиеся высказывают свое мнение, оправдались ли их ожидания от проделанной работы.

Итак, а теперь давайте вспомним все, о чем мы сегодня с вами разговаривали:

1. Что такое вирусы?
2. Каким образом мошенники пытаются «проникнуть» в наш компьютер?
3. Какие меры безопасности нужно соблюдать при работе в сети WiFi.
4. Как вы понимаете понятие «информационный мусор».

Стоит понимать, что сеть Интернет - такой же социум, как и тот, в котором мы все живем. Люди делятся на плохих и хороших. Естественно, хороших гораздо больше, чем плохих, но это не повод для того, чтобы не замечать явных попыток поступать нехорошо и некрасиво с вами. Всем спасибо за урок.

**Краткие правила безопасного использования интернета в стихах:**

1. Иногда тебе в сети вдруг встречаются вруны. Ты мошенникам не верь, Информацию проверь.

2. Не хочу попасть в беду – Антивирус заведу! Всем, кто ходит в интернет, пригодится наш совет.

3. 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!

4. С грубиянами в сети Разговор не заводи. Ну и сам не оплошай, никого не обижай.

5. Злые люди в интернете расставляют свои сети. С незнакомыми людьми Ты на встречу не иди!

6. Как и всюду на планете есть опасность в интернете. Мы опасность исключаем, если фильтры подключаем.

7. Если что-то непонятно, страшно или неприятно, быстро к взрослым поспеши, Расскажи и покажи.

