**Муниципальное бюджетное общеобразовательное учреждение**

**средняя общеобразовательная школа №2**

Конспект урока на тему:

«Интернет: полезно или опасно?»

\_\_Чукалиной Марии Владимировны, без категории\_

Ф.И.О., категория

Информатика

7-8 классы

Предмет, класс

2014-2015 учебный год

**Тема урока: Интернет: полезно или опасно?**

**(7-8 классы)**

**Цель урока**: изучить угрозы сети Интернет и методы борьбы с ними;

**Задачи урока:**

1. формирование представлений о WWW как всемирном хранилище информации;

2. знакомство с понятием: безопасность в сети Интернет;

3. формирование ответственного отношения к информации с учетом правовых и этических аспектов ее распространения;

4. развитие чувства личной ответственности за качество окружающей информационной среды.

**Ход урока.**

**1. Актуализация знаний.**

Всемирная паутина – это мощнейшее информационное хранилище, содержащийся в ней объем информации не поддается точному измерению.

На сегодняшний день практический каждый человек, так или иначе, пользуется сетью Интернет. Возможности Интернет безграничны: учеба, поиск необходимой информации, перевод денежных средств, отдых и многое другое. Однако, многие пользователи даже не задумываются о том, какая опасность поджидает нас во всемирной паутине.

Давайте подумаем и вспомним, какие угрозы вы уже встречали во время работы за компьютером, а может, о каких-то угрозах, вы слышали от своих друзей? (ответы детей).

**2. Объяснение нового материала.**

Сегодня мы с вами погорим о том, как сохранить свои личные данные в сети интернет.

Любой человек имеющий доступ к Интернету, может разместить в сети свою информацию. К этой информации будет иметь доступ весь мир. Но, одно дело поделиться интересным открытием, посоветовать книгу или понравившийся фильм, и совсем другое дело: рассказать по «секрету всему свету» о своём домашнем адресе, номере телефона и уж тем более показать всем фото в паспорте или другие персональные секретные данные.

Мошенники могут быть хорошо оснащены и использовать самые разные инструменты и методы – например, вирусное программное обеспечение, поддельные сайты, мошеннические письма, перехват и подбор паролей к учетным записям в социальных сетях и почтовых сервисах.

Вирусы могут распространяться с помощью вложенных файлов и ссылок в электронных письмах, в сообщениях в социальных сетях, на съемных носителях, через зараженные сайты. При этом сообщение с вирусом может быть получено как от постороннего человека, так и от знакомого, но уже зараженного участника социальной сети или почтовой переписки. Зараженными могут быть сайты, как специально созданные в целях мошенничества, так и обычные, но имеющие уязвимости информационной безопасности.

**Существует несколько правил, которые позволят Вам уберечь себя от мошенников в сети:**

* Использовать антивирусные программы с обновленными вирусными базами.
* Не открывать вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства коммуникаций в интернете, не удостоверившись, что файл или ссылка не содержит вирус.
* Внимательно проверять доменное имя сайта (например, www.yandex.ru), так как злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение (например, www.yadndex.ru).
* Не указывать свой мобильный номер на незнакомых сайтах.
* Не доверять объявлениям о подозрительно дешевых товарах.
* Никому не сообщать свой пароль и т.д.

В Интернете пароль имеет большое значение, и если пароль сложный и надежный, то никто не будет угрожать нашим электронным ресурсам. Надежный пароль, как замок предотвращает вторжение непрошенных гостей, а может быть и злоумышленников.

**Правила создания надежного пароля:**

Идеальный пароль – это длинная комбинация различных знаков, которая включает в себя не только буквы и цифры, а также знаки пунктуации и символы.

* Если это возможно, старайтесь использовать восемь и более знаков.
* Не указывайте в пароле свое имя, фамилию, дату рождения и другие данные, которые находятся в общем доступе в сети.
* Не используйте один и тот же пароль везде. Злоумышленники крадут учетные данные на сайтах со слабой безопасностью, а затем пытаются использовать те же пароли и имена пользователя, чтобы получить доступ к более защищенным ресурсам, например, банковским сайтам.
* Старайтесь регулярно менять свои пароли. Установите автоматическое напоминание, которое будет уведомлять вас о необходимости сменить пароли на используемых вами ресурсах.
* Чем больше разнообразных символов вы используете в пароле, тем лучше. Тем не менее, помните, что программы для подбора паролей автоматически проверяют их на замену распространенных комбинаций букв на символы, например, "to" на "2".
* Следует использовать все имеющиеся на клавиатуре символы, а не только те, которые используются или отображаются чаще всего.

**3. Закрепление.**

А теперь, давайте проверим, насколько внимательно вы сегодня слушали данный материал. (Учащиеся получают тестовые задания).

*Примеры тестов:*

**1. Вам пришло письмо: «Чтобы выиграть миллион в нашей лотерее, вам нужно зарегистрироваться на этом сайте (ссылка на сайт). Регистрация закрывается завтра. Не пропустите!». Что вы сделаете?**

1. Зайду на сайт и посмотрю, что за лотерея.
2. Напишу в ответ письмо, где попрошу прислать подробности о лотерее.
3. Удалю письмо. Я ничего не знаю об этом сайте и авторе письма. Скорее всего, это спам.

**2. Вам пришло письмо «Новые снимки на сервере Яндекс.Фотки. Открой и увидишь!**[**www.fotoyandex123.ru»**](http://www.fotoyandex123.ru)**. Как вы поступите?**

1. Обязательно посмотрю фотографии.
2. Поделюсь ссылкой с друзьями.
3. Удалю письмо. Скорее всего, его прислали мошенники: доменный адрес сайта отличается от настоящего адреса Яндекс.Фоток. Вполне вероятно, что сайт заражен.

**3. ВКонтакте вдруг просит повторно ввести ваши логин и пароль, чего раньше никогда не было.Что вы сделаете?**

1. Введу, раз нужно.
2. Проверю доменный адрес сайта. Если он не совпадает с настоящим, закрою сайт.
3. Введу данные, так как мо аккаунт во Вконтакте привязан к мобильному номеру, а значит, защищен от любого мошенничества.

**4. Как злоумышленник может украсть ваш пароль?**

1. Укажите все верные варианты.
2. Если не записывать пароль на бумаге, то никак.
3. Если пароль достаточно легкий, его можно просто угадать.
4. Злоумышленник может использовать поддельный сайт (например, внешне очень похожий Вконтакте), и заставить меня ввести на нем пароль.

**5. Какой пароль является самым сложным?**

1. Natalia1993
2. Mar1nA@1993
3. verinica93

*Ответы: 1-с; 2-с,3-b; 4-b,c; 5-b.*

**4. Подведение итогов урока.**

**Использованная литература:**

* Методические рекомендации: Методика организации недели «Безопасность. Интернет»./Авторы составители: Селиванова О. В., Иванова И. Ю., Примакова Е. А., Кривопалова И. В. - Тамбов, ИПКРО 2012.
* Мельников В.П. Информационная безопасность и защита информации: учеб.пособие для студентов высших учебных заведений; 3-е изд., стер.-М.: Издательский центр «Академия», 2008. – 336 с.