|  |  |
| --- | --- |
| Автор (ФИО, образовательное учреждение): | Моисеенко Ольга Михайловна, МБОУ СОШ № 167 |
| Название модуля и тема внутри модуля | **Модуль 4. Цифровое потребление.**   * Мошенничество в сети |
| Форма: | фрагмент урока по предмету |
| Класс: | 7 |
| Тема урока | Безопасность в сети Интернет |
| Цель: | знакомство учащихся с видами опасностей, которые могут подстерегать их в сети Интернет |

|  |  |
| --- | --- |
| Задача: | * знакомство учащихся с правилами безопасности в сети Интернет; * развитие у детей чувства осторожности при использовании сети Интернет; * привитие бережного отношения к своим персональным данным. |
| Необходимые медиа материалы: | Видео ролик  *http://www.youtube.com/watch?v=AMCsvZXCd9w* |
| Время проведения: | 45 мин |

**Процедура проведения**

**План урока:**

1. Организационный момент.

2. Объяснение нового материала.

3. Закрепление усвоенного материала.

4. Подведение итогов.

**Объяснение нового материала.**

1. Как и для каких целей используют учащиеся Интернет.

2. Поверхностное знакомство учащихся с видами опасностей в сети Интернет:

1. Вирусы.
2. Мошеннические письма.

3. Знакомство учащихся с видом опасности в сети Интернет, связанным с вирусами:

Вирусы могут распространяться с помощью ссылок и файлов в электронных письмах, в сообщениях, которые мы получаем в социальных сетях (например, «Одноклассники») или Интернет-пейджерах (например, Mail.ru Агент). При этом, стоит относиться к таким случаям внимательно. Подозрительное письмо или сообщение вам может прислать не только посторонний человек, но и ваш друг, компьютер которого уже заражен вирусами. Кроме того, вирусы могут распространяться на съемных носителях («флэшках»).

4. Мошеннические письма:

Следующий вид опасности – это мошеннические письма.

Как правило, злоумышленники в данном случае пользуются различными методами социальной инженерии. То есть собирают какие-то личные данные о жертве, которые имеются в свободном доступе в сети Интернет. На основе полученных данных они пишут письма жертвам по определенному сценарию.

Один из примеров – это когда вы получаете электронное письмо, в котором вам сообщается, что вы выиграли большую сумму денег. Но для того, чтобы получить выигрыш, вам необходимо перечислить на определенный счет нужную сумму. Как правило, вы ничего нигде не выигрывали, и после перечисления денег на счет вы никакого выигрыша не получите.

В последнее время стали распространены случаи мошенничества с использованием не только электронной почты, но и социальных сетей, а также мобильной связи. Например, в социальной сети или на мобильный телефон вашим родителям может прийти сообщение, что с вами что-то случилось, и чтобы предотвратить еще более ужасные последствия, им необходимо перечислить или перевести деньги. На самом деле с вами все может быть в порядке, а ваши родители, не разобравшись в ситуации глубже, срочно переведут деньги на чужой счет.

5. Получение доступа к учетным записям в социальных сетях и прочих сервисах сети Интернет:

Еще один вид опасности – получение доступа к учетным записям в социальных сетях и прочих сервисах.

Многие из вас пользуются социальными сетями? Кто из вас пользуется электронной почтой?

Сейчас очень часто встречается обман в социальных сетях, основанный на том, что за именем и фотографией человека в социальной сети на самом деле может скрываться совсем другой человек. На обман в данных случаях злоумышленник идет часто для последующего совершения преступления.

Как же уберечься от мошенников? Посмотрим ролик, где нам дадут ряд полезных советов.

*Показываю видеоролик, размещенный в сети Интернет по ссылке:**http://www.youtube.com/watch?v=AMCsvZXCd9w*