Автор (ФИО, образовательное учреждение):	Автор (ФИО, образовательное учреждение): Юрина Юлия Николаевна, МАОУ Гимназия № 11 «Гармония»
Название модуля	Модуль 4. Цифровое потребление
Форма:	Внеклассное мероприятие
Класс:	14-15 лет
Тема урока (собрания, выступления и т.д.):	Урок Мошенничество в Сети
Цель:	● Повысить уровень знаний учащихся о мошенничестве в Сети.
Основные вопросы	● Мошенничество в Сети ● Безопасность в Интернете
Необходимые материалы:	Безопасность платежей в интернете https://events.yandex.ru/lib/talks/2481/
Дополнительные материалы по теме:	● Тест «Безопасность в интернете» ● Рефлексия

1. Приветствие.
2. Просмотр видеоролика “Безопасность платежей в интернете” https://events.yandex.ru/lib/talks/2481/.
3. Обсуждение вопросов:
    a. по общей безопасности в интернете;
    b. правил пользования электронной почтой;
    c. признаков фальшивых писем, квитанций, лотерей, сайтов
4. Работа в группах:
    1) составить текст “нигерийских” писем, фальшивых смс для обсуждения участниками другой группы;
    2) обсуждение “опасных” сообщений.
5. Тест “Безопасность в интернете”

6. **Итог урока. Советы** “Как не попасться на удочку?”

К сожалению, недобросовестных людей хватает. Мошенники и аферисты буквально в каждой сфере деятельности находят своих «клиентов». Не стала исключением и всемирная глобальная сеть. Мошенников в интернете – десятки и сотни тысяч, как же не попасться на их удочку?

Предупрежден – значит, вооружен. Поэтому чтобы оградить себя, необходимо, прежде всего, выяснить, какими же способами пользуются интернет-мошенники для обмана доверчивых пользователей?

Способ №1

На ровном месте мошенники предлагают заработать миллионы. Что для этого нужно? Всего лишь приобрести у них чудо-программу, которая способна генерировать пин-коды пластиковых карт, например, или коды карт пополнения счета.
На самом деле, конечно, предлагаемая мошенниками программа ничего подобного не делает. В лучшем случае это генератор случайных чисел, а в худшем – какой-нибудь компьютерный вирус.

Еще одна разновидность этого способа – это программы-взломщики или перехватчики информации. Мошенники даже могут написать столь убедительную инструкцию к программе, что непосвященному пользователю она покажется эффективной.

Безусловно, опытные хакеры действительно пишут для себя подобные программы. Однако, во-первых, взлом – это незаконно. А во-вторых, стоит задуматься: почему такую «золотую жилу» мошенник предлагает другим пользователям?

Способ №2

Мошенники предлагают пользователю заработать на просмотре рекламы: кликать на баннеры и получать за это деньги. Это не криминал, но и много денег таким способом заработать не удастся.

Чтобы пользователь мог вывести заработанные деньги из системы, мошенники предлагают ему купить у них «ноу-хау» за определенную сумму. Но так как изначально никто и не собирался пользователю ничего платить, то, естественно, никакого «ноу-хау» быть не может.

Способ №3

«Волшебные кошельки» - старый добрый способ интернет-мошенничества. Пользователю предлагают перевести небольшие суммы на определенные электронные кошельки и затем получить свои деньги в удвоенном размере. Доверчивый пользователь в

порыве азарта отправляет с каждым разом все большую сумму, но назад никаких денег больше не получает.

Во втором варианте «волшебных кошельков» мошенники предлагают «разорить систему», переводя на кошельки только маленькие суммы. Естественно, что никакой «системы» нет, мошенники просто забирают деньги себе.

Способ №4

Некоторым мошенникам лень изобретать изощренные аферы. И они просто попрошайничают деньги в интернете. Просьбы мошенников могут быть самыми разными: от простых, вроде «дайте на пиво», до слезных историй о несчастной судьбе.

Как правило, подобные истории – чистой воды фантазия. Можно даже дать автору несколько центов за писательский талант и пару минут здорового смеха. Однако мошенники прибегают и к более гнусному обману. Например, просят перевести деньги на лечение больного ребенка или помочь сиротам и бездомным.

Пользователям важно помнить, что информация о реальных благотворительных акциях и их организаторах находится в открытом доступе, есть специальные благотворительные счета в банке, а не электронные кошельки.

Способ №5

Наглый шантаж и угрозы. Пользователю приходит письмо от «администрации» платежной системы, социальной сети или другого ресурса, в котором говорится о необходимости срочно уплатить определенную сумму. В противном случае пользователю угрожают блокированием его аккаунта.

Возможен также вариант, когда пользователя просят выслать на определенный адрес свои регистрационные данные, в том числе логин и пароль от учетной записи.

Способ №6

Фишинг. Пользователю приходит письмо с просьбой войти в свой аккаунт на сайте платежной системы и дается ссылка для перехода. Однако при переходе по этой ссылке пользователь попадает вовсе не на сайт своей платежной системы, а на очень похожую подделку.

Введя свои данные на этом сайте, пользователь видит какую-то ошибку, после чего он автоматически перенаправляется на настоящий сайт. А тем временем данных, которые были введены в форму, уже ушли к мошенникам. Через некоторое время со счета пользователя исчезают деньги.

Адрес фальшивого сайта всегда содержит в своем доменном имени какую-то ошибку, отличающую его от настоящего сайта. Поэтому, чтобы распознать такое

мошенничество, необходимо быть предельно внимательным к различным просьбам ввести свои данные.

Источник **http://strana-sovetov.com/computers/internet/2443-internet-fraud.html**

7. Рефлексия

- было интересно…
- было трудно…
- я понял, что…
- урок дал мне для жизни…
- мне захотелось…