«Виртуальные ловушки и правила безопасной работы в сети Интернет по управлению своими финансовыми средствами»

Участники: учащиеся 9 класса

Цель: Актуализация вопросов финансовой грамотности учащихся, развитие

компетенций, необходимых для грамотного и безопасного поведения в финансово экономической сфере и в сети Интернет.

Задачи:

-развитие мотивации учащихся к повышению собственной финансовой

Грамотности, безопасности и повышение уровня осведомленности в различных областях финансовой грамотности;

-формирование у учащихся компетенций, связанных с поиском информации,

анализом и планированием безопасного управления собственными финансовыми ресурсами;

-развитие у старшеклассников ответственности, творческого потенциала, социальной активности, коммуникативной компетентности в контексте обеспечения финансового благополучия и экономической безопасности .

Подготовительная работа: подготовить для каждого учащегося памятки

Теория:

Оплата услуг и покупка товаров через сеть Интернет происходит разными способами:

* с использованием **электронного кошелька**;
* с использованием **банковской карты**;
* перечислением средств **со счёта мобильного телефона**.

При совершении этих операций платёжные реквизиты **могут быть похищены**!

Виртуальные ловушки в сети Интернет

Существует множество **виртуальных ловушек**в сети Интернет.

**Развитие технологий приводит к появлению всё новых и новых виртуальных ловушек, но на данный момент наиболее распространёнными являются:**

* **фишинг;**
* **фарминг;**
* **скандинавский аукцион;**
* **«семь кошельков»;**
* **лже-интернет-благотворительность.**

Мошенники **получают платёжные реквизиты**и **переводят деньги**с банковских карт и электронных кошельков пользователей сети Интернет.

Условно выделяют два основных способа получения платёжных реквизитов пользователей: **фишинг**и **фарминг**.

**Фишинг — это схема похищения платёжных реквизитов с использованием поддельных сайтов, на которых пользователь сам вводит свои данные.**

Пользователя «заманивают» в неизвестный интернет-магазин и, когда он хочет совершить покупку, перенаправляют его по поддельной ссылке не на сайт его банка, а на похожий поддельный сайт, где пользователь вводит свои платёжные данные и таким образом передаёт их мошенникам.

Для того чтобы защититься от фишинга, необходимо:

* пользоваться сайтами только проверенных интернет-магазинов;
* перед введением информации с банковской карты внимательно изучать адресную строку сайта в браузере;
* адресная строка сайта, на странице которого необходимо ввести платёжные реквизиты, должна начинаться с http:// или https://;
* не вводить платёжные реквизиты, если адрес сайта в адресной строке браузера вызывает сомнения.

**Фарминг — это схема похищения платёжных реквизитов при помощи вредоносного программного обеспечения.**

**Вирус**, попадая на компьютер, планшет или телефон пользователя, **передаёт платёжные реквизиты мошенникам**.

Для того чтобы защититься от фарминга, необходимо использовать лицензионный антивирус на всех устройствах, подключённых к сети Интернет.

**Скандинавский аукцион**— это **способ «почти честного» отъёма денег**в сети Интернет.

**В аукционе побеждает тот, кто назовёт цену последним. В скандинавском аукционе побеждает тот, кто сделает ставку, и если после него в течение**30**минут ставок не будет.**

Ставка (или шаг аукциона) может быть разной (к примеру, 25 коп.). За право сделать ставку, то есть возможность стать последним и приобрести товар, нужно заплатить стоимость шага (к примеру, 10 руб.).

*Обрати внимание!*

Доказать мошенничество в скандинавском аукционе практически невозможно, поскольку реальные люди, являющиеся участниками, **добровольно** делают выплаты. Но кроме реальных людей в скандинавском аукционе принимают участие **роботы**, чья задача — не дать аукциону закончиться.

**Одним из видов мошенничества в сети Интернет является схема под названием «семь кошельков», когда пользователь получает письмо с предложением перевести небольшую сумму на несколько электронных кошельков в надежде на то, что следующие участники тоже перечислят деньги на электронные кошельки, среди которых будет указан и его электронный кошелёк.**

**Гарантия получения денег в свой электронный кошелёк полностью отсутствует**, таким образом, человек добровольно отдаёт некоторую сумму мошенникам.

**Лже-интернет-благотворительность — это схема мошенничества, связанная с распространением поддельных сообщений о сборе средств на благотворительные цели.**

Мошенники зачастую **копируют**информацию **о реальных людях**, **нуждающихся в помощи**, копируют оформление сайтов благотворительных фондов, **заменяя** при этом **платёжные реквизиты на собственные**. Таким образом, пожертвованные средства поступают не на заявленные цели, а в личный кошелёк мошенника.

*Обрати внимание!*

Доказать факт мошенничества бывает крайне трудно, поскольку перевод средств обманутые граждане совершают **добровольно**.

2. Практическая часть. Решение тестовых задач на странице https://www.yaklass.ru/p/osnovy-finansovoj-gramotnosti/7-9-klass/riski-i-finansovaia-bezopasnost-159624/virtualnye-lovushki-ili-kak-ne-poteriat-dengi-v-seti-internet-159210/re-df747c30-e039-4f19-8d7e-c7f6c7c0640f/pe?resultId=3617317050&c=1

Начало формы

**Выбери вариант, наиболее точно соответствующий утверждению**.

1.Современные финансовые пирамиды переместились в сеть Интернет, поскольку Интернет предоставляет организаторам финансовых пирамид ряд преимуществ, одно из которых:

* необходимо отчитываться перед вкладчиками о результатах работы финансовой организации
* необходимо платить налоги с доходов
* организаторы финансовых пирамид в сети Интернет избавлены от необходимости вести бухгалтерскую документацию

Конец формы

2. **Отметь верный вариант**.

Схема похищения платёжных реквизитов, которые крадутся с компьютера пользователя при помощи вредоносного программного обеспечения, называется...

* коучинг
* фарминг
* таргетинг

3. Новый смартфон был продан на скандинавском аукционе за 1884 руб. Рассчитай, сколько участников должны были сделать ставки, если шаг аукциона — 24 коп.

Ответ:  участников.

Какую сумму получил владелец скандинавского аукциона от продажи смартфона, если стоимость шага — 17 руб.?

Ответ:  руб.

4. Шаг скандинавского аукциона равен 25 коп.  
Стоимость шага равна 19 руб.  
Товар стоимостью 36678 руб. был продан на скандинавском аукционе за 1685 руб.  
В аукционе принимали участие не только реальные люди, но и робот, который сделал 1685 шагов. Чему равны общие затраты реальных участников скандинавского аукциона?

Всего в аукционе было сделано  шаг(-а, -ов).

Число шагов, сделанных реальными людьми, равно .

Общие затраты реальных участников аукциона составили  руб.

Таким образом, организаторы продали товар на  руб. дешевле, но получили за этот товар на  руб. больше.

5 Письмо, в котором содержится приглашение перевести деньги в «семь кошельков», получили 47005 человек(-а). Из них 0,25 % откликнулись на это приглашение и перевели на каждый из электронных кошельков по 14 руб.

Какой доход получили мошенники?

*(Ответ округли до десятых.)*

Ответ:  руб.

Сколько потратил человек, откликнувшийся на письмо?

Ответ:  руб.

Какую сумму получил человек, откликнувшийся на письмо?

Ответ:  руб.

6. Представь, что Вася привёл в некий финансовый проект в сети Интернет Петю и Ивана. Петя привёл в проект Олю и Полину, а Иван смог привести в проект Софью и Романа.

Каждый участник сделал взнос в размере 20000 руб. Тому, кто привёл нового участника, выплачивается 20 % от взноса.

Сколько получит Иван?

Ответ:  руб.

Сколько затратил Иван для того, чтобы вступить в проект?

Ответ:  руб.

Сколько человек нужно привлечь Ольге, чтобы оправдать затраты от вступления в проект?

*(Ответ округли до целого числа.)*

Ответ:  человек(-а).

Есть ли гарантия того, что Ольге перечислят деньги?

* Да
* Нет

7. Организаторы финансовой пирамиды запланировали получить доход в размере 2500000 руб.

25 % собранных средств направляется на выплаты тем, кто привёл новых участников пирамиды, 10 % собранных средств направляется на выплаты остальным участникам пирамиды, а остальные — организаторам пирамиды.  
Рассчитай, сколько времени может работать финансовая пирамида, если ей удаётся привлечь в день 50000 руб.

После выплаты процентов вкладчикам организаторам останется  % дохода.

Для того чтобы организаторы смогли получить доход 2500000 руб., им необходимо привлечь в пирамиду денежные средства на сумму (*ответ округли до единиц*)  руб.

Подобная пирамида может работать до (*ответ округли до единиц*)  дн(-я, -ей).

8. **Отметь верный вариант**.

Как защититься от финансового мошенничества в сети Интернет?

Ответ:

* украсть деньги через Интернет невозможно
* подбирать надёжные пароли
* изучать банковские выписки и перечень совершённых операций с банковской карты

9.О**тметь верный вариант**.

Услуги и товары можно оплачивать в сети Интернет различными способами, например...

* дивидендами
* процентами
* с использованием электронного кошелька

Ответить!

Конец формы

10. Начало формы

**Отметь верный вариант**.

Правила безопасной работы в сети Интернет:

* при работе с банкоматом и при оплате банковской картой в магазине закрывать рукой клавиатуру
* антивирус — пустая трата денег
* использовать только официальные приложения

Ответить!

Конец формы

3. Подведение итогов

Безопасная работа в сети Интернет

Для того чтобы защититься от финансового мошенничества в сети Интернет, необходимо:

* **менять пароли**не реже одного раза в месяц;
* для компаний: компьютер, на котором хранится бухгалтерская информация, **не подключать к сети Интернет**;
* **изучать банковские выписки**и перечень совершённых операций с банковской карты;
* подбирать **надёжные пароли**;
* завести **отдельную банковскую карту**для оплаты покупок через сеть Интернет;
* **не хранить средства**на карте для совершения покупок через сеть Интернет, переводить на неё средства только для совершения покупки;
* при обнаружении операции, которую не совершали, **срочно обратиться в банк**с заявлением.

Дополнительной защитой интернет-платежей является использование **технологии 3-D Secure**. По правилам 3-D Secure, интернет-платежи с карты нужно дополнительно подтверждать. Обычно банк присылает одноразовый пароль в СМС, иногда выдаёт карточку с набором кодов, совсем редко назначает постоянный пароль. Информация о технологии **3-D Secure**размещена в разделе «[Польза и риски банковских карт](http://www.yaklass.ru/p/osnovy-finansovoj-gramotnosti/7-9-klass/bankovskaia-i-nalogovaia-sistemy-127377/polza-i-riski-bankovskikh-kart-127386/re-63ae8749-f7c0-4299-9d57-3ab970e664ef)».

**Правила безопасной работы в сети Интернет:**

* **не сообщать никому, даже сотрудникам банка, свои пароли и ПИН-коды от банковских карт;**
* **использовать антивирус не только на компьютере, но и на мобильном телефоне и планшете;**
* **не переходить по ссылкам, присланным в социальных сетях и по электронной почте;**
* **использовать только официальные приложения;**
* **при работе с банкоматом и при оплате банковской картой в магазине закрывать рукой клавиатуру;**
* **пользоваться СМС-оповещением о совершённых операциях с банковской карты;**
* **не использовать сомнительные сайты;**
* **помнить правило «бесплатный сыр бывает только в мышеловке» и не отвечать на письма о выигрышах.**

При совершении оплаты на сайте нужно внимательно посмотреть на адресную строку:

1. страница ввода данных**защищена по протоколу SSL/TLS**: адрес сайта будет начинаться на **https://**;
2. в адресной строке должна быть надпись «**Защищённый режим**» и значок «**замочек**»;
3. должно насторожить, если адрес сайта является доменом третьего уровня, например: [**www.МАГАЗИН.XXXX.ru**](http://www.xn--80aairftm.xxxx.ru/);
4. нужно знать, что на сайте **nalog.ru**можно проверить, **зарегистрирована ли компания с таким названием и ИНН и существует ли она на данный момент**.

