Проект

Методика и содержание внеурочного занятия по теме “Виртуальные ловушки, или как не потерять деньги в сети интернет”

Группа №4:

Казаченко Наталья Сергеевна

Коровянская Оксана Викторовна

Тетусь Ольга Вячеславовна

Гаврилова Елена Юрьевна

ЦЕЛИ И ЗАДАЧИ ПРОЕКТА

Цели проекта:

Изучить виды виртуальных ловушек и способов безопасной работы в сети интернет

Задачи:

1. Рассмотреть организацию финансовых пирамид в сети интернет;
2. Познакомиться с основными видами виртуальных ловушек (фишинг, фарминг, скандинавский аукцион).
3. Разработать правила безопасного поведения в сети интернет;

Планируемые результаты

1. Знания об организации виртуальных ловушек и правила защиты от них.
2. Правила безопасной работы в сети интернет.

Введение

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:

1. фишинг;
2. фарминг;
3. скандинавский аукцион;
4. «семь кошельков»
5. 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**.

1. **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.

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

Вирус, попадая в 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.

3. **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 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.).

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.

4. Одним из видов мошенничества в сети Интернет является схема под названием **«семь кошельков»**, когда пользователь сети Интернет получает письмо с предложением перевести небольшую сумму в 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 кошелек полностью отсутствует, таким образом человек добровольно отдаёт некоторую сумму мошенникам.

5. **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.

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

Вывод

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».

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 в банкомате и при оплате банковской картой в магазине закрывать рукой клавиатуру.
- Пользоваться SMS-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.
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.