КОМИТЕТ ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ ВОЛГОГРАДСКОЙ ОБЛАСТИ
ГБПОУ «ФРОЛОВСКИЙ ПРОМЫШЛЕННО-ЭКОНОМИЧЕСКИЙ ТЕХНИКУМ»

Индивидуальный исследовательский проект
по учебной дисциплине
ОБЩЕСТВОЗНАНИЕ
Тема: Интернет мошенничество

Выполнил:
студент гр. А-20
Мурзин Максим Витальевич
Руководитель проекта:
преподаватель
Панченко Наталья Александровна

Фролово, 2021

Введение

- Актуальность: Я считаю, что тема интернет-мошенничества в наше время очень важна т.к. в наше время большинство действий происходят в интернете и многие люди даже не представляют, как работают интернет-мошенники, и не знают в какой момент их могут обмануть.
- Цель: выяснить что такое интернет-мошенничество и какие есть методы борьбы с ним
- Задачи:
  1.Изучить доступную литературу и интернет источники.
  2.Проанализировать и обобщить полученные знания.
  3. Отобрать для проекта наиболее интересный материал.
  4. Оформить презентацию по данной теме.
  5.Защита проекта.

Что такое интернет мошенничество

Интернет-мошенничество — вид мошенничества с использованием Интернета.
Оно может включать в себя сокрытие информации или предоставление неверной информации с целью вымогательства у жертв денег, имущества и наследства.

Виды интернет-мошенничества

На данный момент существует огромное количество видов интернет-мошенничества, которые отличаются тем, что направлены на какую-либо целевую аудиторию(например: любителей халявы, любителей концертов).

Существуют такие виды интернет-мошенничества как:

- Мошенничество с благотворительностью
- Мошенничество с билетами
- Мошенничество с подарочными картами
- Фишинг
- Вирусы
- Взлом электронных кошельков

Мошенничество с благотворительностью

Мошенник прикидывается представителем благотворительной организации, собирающей средства на помощь жертвам стихийного бедствия, террористической атаки, регионального конфликта или эпидемии.

Также средства могут собирать без привязки к конкретному событию, а, например,

на исследования рака, СПИДа или вируса Эбола, детские приюты. Мошенники могут выдавать себя за такие благотворительные организации, как Красный Крест или ООН. Мошенник просит пожертвований, часто ссылаясь на новостные статьи в Интернете, чтобы подкрепить свою историю о сборе средств. Жертвы таких мошенников — это благотворительные люди, которые верят, что помогают достойному делу, и ничего не ждут взамен.

Мошенничество с билетами

Мошенничество с билетами является одной из разновидностей мошенничества в интернет-маркетинге. Злоумышленники предлагают билеты на популярные мероприятия, такие как концерты, шоу и спортивные мероприятия. В результате билеты являются поддельными или не доставляются покупателям.

Распространение онлайн-агентств по продаже билетов и существование опытных и нечестных продавцов билетов подпитывают этот вид мошенничества. Многие из таких мошенников управляются британскими билетными рекламодателями, хотя они могут базировать свои операции в других странах

Мошенничество с подарочными картами

Последнее время преступники всё чаще занимаются мошенничеством с использованием подарочных карт магазинов. В частности, злоумышленники пытаются получить информацию, касающуюся подарочных карт, которые были выпущены, но не были использованы.

Сначала хакеры крадут данные подарочной карты, проверяют существующий баланс через онлайн-сервис магазина, а затем пытаются использовать эти средства для покупки товаров или перепродажи на стороннем веб-сайте.

В случаях перепродажи подарочных карт злоумышленники забирают оставшуюся сумму наличными, что также можно использовать как метод отмывания денег.

Фишинг

вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам

Вирусы

Чтобы получить информацию от пользователя нужную информацию, аферисты используют разного рода "приманки". Одних обещают научить читать чужие сообщения, другим предлагают рассказать о способе повышения рейтинга в социальной сети, третьим рекламируют программы для взлома SMS. Чтобы получить обещанное, пользователь должен перейти по предложенной ссылке на специальный сайт. Там, в свою очередь, потребуют номер телефона или логин с паролем от соц сети. Если нужная информация будет предоставлена, то в первом случае счёт человека на мобильном обнулится, а во втором - исчезнет доступ к аккаунту.

Взлом электронных кошельков

Пользователю приходит SMS или электронное письмо с требованием предоставить учётные данные кошелька - например, для его разблокировали. Могут быть названы и другие виды причин, но сути дела это не меняет. Главное для интернет-мошенников - получить доступ к вашему кошельку с целью снятия с него денег.

Как не стать жертвой интернет-мошенничества

1. Не ищите легкую наживу. Быстрого заработка в интернете не существует. Объявление с фразой «заработок в интернете без вложений» значит, что вас осторожно заманивают в финансовую пирамиду или мошенническую сеть. Таких в интернете много, и есть даже курсы, которые обучают новичков создавать в интернете филиалы мошеннических сетей.
2. Придумайте сильный пароль. В качестве пароля от интернет-банка поставьте любой набор цифр, букв, смайликов и знаков препинания. Лучшие пароли придумывают коты, когда ходят по клавиатуре. Проще восстановить пароль, чем вернуть украденные деньги.
3. Научитесь использовать VPN. Если за сетью кафе или аэропорта следит жулик, то ваши пароли, интимные фото и переписка на сайте знакомств находятся под угрозой. Мошенник может осторожно выкачать из компьютера компромат, а потом начнет вас шантажировать. Чтобы он не смог узнать ваши тайны, всегда используйте VPN в незнакомых местах

Что делать, если стал жертвой интернет-мошенников?

Если вы подозреваете, что стали жертвой мошенников, немедленно позвоните в банк и заблокируйте карту. После этого сообщите о мошенниках — даже в том случае если никаких сомнительных операций еще не произошло, а вы просто сообщили номер своей карты неизвестно кому. Лучше быть параноиком, чем без денег. Разные банки по-разному реагируют на вопросы мошенничества. Где-то можно написать в интернет-чате или позвонить по телефону кол-центра, где-то придется ехать в банк и писать заявление. Заявление об интернет-мошенниках и ложной операции необходимо отправить как можно раньше — в идеале сразу же. Максимум — в течение суток. Если вы опоздаете, то банк может отказать в проведении расследования.

Куда сообщить о мошенниках?

Чтобы поймать преступников по горячему следу, лучше сразу обратиться в ближайшее отделение полиции по месту жительства. Чем быстрее вы сообщите о преступлении, тем больше шансов наказать мошенников. Но если вы боитесь потратить время и ничего не добиться, то хотя бы отправьте электронное обращение в управление «К» МВД России.Если у мошенников есть сайт, то наказать их еще проще. Можно сразу сообщить о вредоносном сайте, чтобы его заблокировали. Даже если преступников не получится поймать, вы сохраните деньги других пользователей. Чтобы сообщить о мошеннических сайтах обратитесь в поддержку Google или Яндекс

Закючение

В процессе работы над данным проектом, я узнал о различных видах интернет-мошенничества и о том, как не стать жертвой мошенников, научился обобщать информацию и правильно оформлять проект. Считаю, что цель моей работы достигнута, я выяснил что такое интернет-мошенничество и какие есть методы борьбы с ним. В процессе работы над проектом я столкнулся с такой проблемой как недостаток литературы по этой теме.

Список литературы и интернет-источников

1. https://journal.tinkoff.ru/wiki/fraud/
2. https://sales-generator.ru/blog/vidy-moshennichestva-v-internete/
3. https://yandex.ru/turbo/avisi.ru/s/osnovnye-vidy-internet-moshennichestva.html
4. https://ru.wikipedia.org/wiki/Фишинг