МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ГОРОД КРАСНОДАР СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 70 ИМЕНИ ГЕРОЯ СОВЕТСКОГО СОЮЗА ДМИТРИЯ МИРОШНИЧЕНКО

Проектно-исследовательская работа

Тема: «Мошенничество в сети интернет»

Выполнил:

Учащийся 11 «А» класса

МАОУ СОШ № 70

Семиженов Д.М

Куратор:

Учитель по информатике

Шиманская Е.Е

Краснодар,2023

Введение

Актуальность работы: В современном мире мы все больше проводим времени в Интернете, там большая часть нашей работы, вся информация и связь с людьми, нам стало привычно находить всю информацию в сети. Мы совершаем покупки по Интернету и это стало совсем обычным делом. Но одновременно с этим развивается и мошенничество в Интернете. Поэтому я считаю, что эта проблема достаточно актуальна в наши дни.

Цель: Создать рекомендации по безопасному использованию сети Интернет, сделав из них буклет. Проинформировать учеников нашей школы, а они в свою очередь проинформировали своих близких людей.

Задачи:

* Рассмотреть историю появления мошенничества.
* Влияние мошенничества на пользователей Интернета
* Виды мошенничества
* Способы борьбы с мошенничеством

Объект исследования: Объектом исследования данной научной работы являются общественные отношения, складывающиеся при совершении мошенничества, предметом - изучение которого является целью данной статьи, — способы мошенничества в сети Интернет, как одного из элементов криминалистической характеристики данного вида преступлений.

Гипотеза: Избежать обмана в сети вполне вероятно, если пользователи будут хорошо проинформированы.

1. История появления.

Мошенничество в интернете существует уже довольно долгое время, но с распространением интернета и развитием технологий, оно стало гораздо более распространенным и сложным. Вот история его возникновения: 1990-е годы: В начале 1990-х годов интернет был еще относительно новым явлением, и мошенничество тоже только начинало развиваться. Основная проблема в то время заключалась в незаконном доступе к компьютерным системам и вирусных атаках. Хакеры и вирусологи стали первыми мошенниками в онлайне, крадя личные данные и нарушая безопасность компьютеров пользователей. 2000-е годы: С развитием интернет-торговли и массовым появлением интернет-банкинга в 2000-х годах, мошенничеству удалось достичь новых высот. Фишинг, которым начали пользоваться мошенники, был одним из наиболее распространенных способов кражи личных данных и паролей. Также стали популярными фейковые онлайн-магазины и странички, обманывающие пользователей и продающие фальшивые товары. 2010-е годы: С развитием социальных сетей и мобильного интернета, мошенничество в интернете стало еще более распространенным. Социальная инженерия и фишинг стали все более изощренными, а мошенники начали использовать новые технологии, такие как искусственный интеллект и автоматизированные системы для обмана пользователей. Онлайн-вымогательство также стало крупным преступлением, когда мошенники шифруют данные пользователей и требуют выкуп за их возврат. В настоящее время мошенничество в интернете является одной из крупнейших угроз для пользователей. Оно принимает много форм и постоянно эволюционирует, чтобы обмануть людей и получить доступ к их личной информации, финансовым средствам и другим ресурсам. Пользователям следует быть осторожными и принимать все необходимые меры для защиты своих данных и себя от мошенников.

2.Виды мошенничества

2.1 Интернет-попрошайничество

Интернет-попрошайничество - это явление, при котором люди или организации используют интернет для просьбы о деньгах или другой помощи. Это может быть выполнено через социальные сети, форумы, блоги, электронную почту или специальные платформы для сбора средств, такие как «Кикстартер» или «GoFundMe». В некоторых случаях интернет-попрошайничество может быть оправданным, например, когда люди собирают средства на лечение или помощь нуждающимся. Однако, существуют и случаи злоупотребления и мошенничества. Некоторые люди могут создавать фальшивые истории и использовать их для мошенничества и получения денег от добрых незнакомцев. Для того чтобы избежать стать жертвой интернет-попрошайничества, важно быть осторожными и проверять достоверность историй и просьб о помощи. Стоит обратить внимание на сомнительные схемы сбора средств и личные данные, а также обратиться к официальным организациям или сайтам для подтверждения и проверки просьбы.

 2.2 Фальшивые антивирусы

Фальшивые антивирусы - это программы, которые претендуют на роль антивирусных программ, но на самом деле являются вредоносным ПО. Они могут выдавать ложные предупреждения о наличии вирусов на компьютере и предлагать пользователю приобрести полную версию программы для удаления этих вирусов. Цель фальшивых антивирусов - обмануть пользователей и заставить их заплатить за несуществующие услуги. После того, как пользователь оплачивает программу, ему могут предложить установить другие вредоносные программы или украсть его личные данные. Чтобы защититься от фальшивых антивирусов, рекомендуется использовать надежные, известные антивирусные программы от проверенных разработчиков. Также следует быть осторожным при установке программ и не доверять предупреждениям о вирусах, поступающим от неизвестных и ненадежных источников.

2.3 Фишинг

Фишинг (пишется также как "фишинг" или "фишинговая атака") - это вид кибератаки, при которой злоумышленники пытаются получить доступ к чувствительной информации (такой как пароли, номера кредитных карт, персональные данные) путем маскировки под доверенную организацию или личность и обманывая пользователей. Обычно, фишинг-атака происходит через электронную почту, сообщения в социальных сетях или мессенджерах. Злоумышленники отправляют ложные запросы, требуя от пользователя предоставить свои логины, пароли или другую конфиденциальную информацию, часто с помощью подделанных веб-сайтов или приложений.

Важно помнить, что поддержка и финансовые организации, а также другие сервисы, никогда не запрашивают у пользователей пароли или другую конфиденциальную информацию путем электронной почты или сообщений. Если вы получили подозрительное сообщение, лучше связаться с организацией напрямую, чтобы удостовериться в его легитимности.

2.4 Кардинг

Кардинг - это незаконная деятельность направленная на получение денег или материальных благ путем злоупотребления кредитными или дебетовыми картами. Кардеры (люди, занимающиеся кардингом) используют различные методы, такие как кража личных данных, взлом сайтов или торговых платформ, фальшивые банковские операции и т. д., чтобы получить доступ к чужим финансовым средствам. Кардинг считается преступлением, и за его совершение могут быть предусмотрены серьезные наказания, включая тюремное заключение.

2.5 Программы – пустышки, обманщики, фейки

Специалисты компании «Доктор Веб» – российского разработчика средств информационной безопасности – выявили сеть из более чем 20 поддельных торрент-трекеров и файлообменников, созданных злоумышленниками за последние несколько недель для реализации их мошеннических схем. Несмотря на формальную бесплатность, при запуске скачанного с такого сайта файла требуется отправить несколько платных SMS-сообщений. Однако даже после этого запрашиваемый фильм, музыкальная композиция или книга пользователю не достаются. Зачастую такие сайты занимают первые места в поисковых системах, что увеличивает аудиторию потенциальных жертв.
 На сегодняшний день сеть поддельных торрент-трекеров и файлообменников, появившихся в Рунете, является весьма обширной. В нее входит более 20 сайтов, зарегистрированных с 8 марта по 14 апреля 2010 года.

3.Наказание

Наказание за мошенничество в Интернете может различаться в зависимости от законов и юрисдикции, в которой происходит преступление. В большинстве стран существуют законы, предусматривающие наказание за интернет-мошенничество, такие как мошенничество с использованием кражи личных данных, кредитных карт, фишинг, незаконный доступ к компьютерной информации, создание фальшивых онлайн-магазинов и другие виды мошенничества.

Наказание за интернет-мошенничество может включать:

3.1. Штрафы: наложение денежного взыскания за совершенное преступление.

3.2. Ограничение свободы: в виде ареста или ограничения свободы передачи данных.

3.3. Условное осуждение: когда суд может назначить осужденному срок наказания, который будет применяться, только если человек нарушит определенные условия.

3.4. Условно-досрочное освобождение: когда осужденному назначается некий срок наказания, но после определенного времени он может быть освобожден с условием дальнейшего контроля и поведения.

3.5. Реабилитационные программы: осужденным может быть предложено участие в программе реабилитации для повышения шансов на успешное социальное возвращение.

3.6. Пожизненное заключение: в случае особо тяжких преступлений или рецидивистов, суд может назначить пожизненное заключение.

Важно отметить, что конкретное наказание будет зависеть от сути и тяжести преступления, совершенных уголовных деяний и предыдущей судимости лица.

4. Как обезопасить себя

Есть несколько способов защиты от мошенничества:

Проверяйте ссылки перед их открытием: Удостоверьтесь, что ссылки, на которые вы нажимаете, действительно приводят к надежным сайтам. Избегайте кликать на подозрительные ссылки в письмах или на непроверенных сайтах. Используйте надежные пароли: Создавайте уникальные и сложные пароли для каждого аккаунта. Используйте менеджеры паролей для безопасного хранения и управления паролями. Обновляйте программное обеспечение: Регулярно обновляйте операционные системы и приложения, чтобы исправить уязвимости, что поможет защитить ваше устройство от вредоносных атак. Используйте антивирусное программное обеспечение: Установите надежное антивирусное программное обеспечение на свои устройства, чтобы обнаруживать и блокировать вредоносные программы. Будьте осторожны при общении в сети: Избегайте предоставления личной информации в сети, особенно на ненадежных сайтах или в ответ на подозрительные запросы. Станьте осведомленным об угрозах безопасности: Ознакомьтесь с актуальными методами защиты от фишинга, социальной инженерии и других видов кибератак. Используйте двухфакторную аутентификацию: Включите двухфакторную аутентификацию, где это возможно, чтобы повысить безопасность своих аккаунтов

Заключение
Мошенничество, увы, неискоренимо. И на просторах Интернета оно

подстерегает нас везде: в электронной почте, социальных сетях, на

различных сайтах. С годами злоумышленники изобретают новые приемы, но

основные механизмы обмана не меняются. Только сам пользователь может

сделать свою жизнь в виртуальном пространстве безопасной. Мы надеемся,

что предоставленная информация будет вам полезна.

В исследовательской работе я представил лишь мизерную долю того

многообразия видов мошенничества, что есть в Интернете. Если описывать все

варианты, то получится целая книга из нескольких томов!

У меня была цель не только перечислить и описать способы отъема денег

при помощи Интернета, а донести до вас, что никто просто так в Интернете

денег не дает. Не стоит верить в обещания об огромных заработках уже через

неделю, реальная работа в Интернете – это действительно работа в полном

смысле этого слова. Есть много честных способов заработка при помощи

Интернета, они требуют усилий и времени.

Изучив результаты анкетирования, мы пришли к выводам, что не

каждый знает об опасностях, подстерегающих их на просторах сети

Интернет.

Список литературы:

1. «Мошенничество в Интернете. Методы удаленного выманивания денег, и как не стать жертвой злоумышленников.» Автор: Алексей Гладкий

2. «Как я украл миллион. Исповедь раскаявшегося кардера.» Автор: Сергей Павлович.

3. <https://apni.ru/>

4. <https://lifehacker.ru/>

5. «Информатика». А. С. Грошев, П. В. Закляков

6.Мартина Доув: «Психология мошенничества. Методы убеждения и мошенничества»

7. <https://cisoclub.ru/>

8. <https://sales-generator.ru/>