Муниципальное бюджетное общеобразовательное учреждение муниципального образования город Краснодар

средняя общеобразовательная школа №70

 Имени Героя Советского Союза Дмитрия Мирошниченко

ПРОЕКТНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА

ПО ТЕМЕ:

«Мошенничество в интернете. Способы борьбы с ним»

|  |  |
| --- | --- |
|  | *Работу выполнил: Хвостов Михаил Сергеевич**Класс:11«В»,\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* *(подпись)**Куратор**Хвостова Татьяна Станиславовна, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*  *(подпись)**Нормоконтролёр,**Хвостова Татьяна Станиславовна, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*  *(подпись)* |

Краснодар, 2024

СОДЕРЖАНИЕ

ВВЕДЕНИЕ................................................................................................................

1. Глава 1……….………………………………………………………….............5

1.1 Современные виды онлайн-мошенничества………………………………...5

1.2 Изучение реальных случаев…………………….…………………………..6

2. Глава 2…………….............................................................................................8

2. Обзор существующих методов и технологий по борьбе с кибер-преступностью…………………………………..…….......................................8

ЗАКЛЮЧЕНИЕ…………………………………………………………………….

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ…………………………………...

ВВЕДЕНИЕ

В современном цифровом обществе, где интернет является неотъемлемой частью нашей жизни, мошенничество и инфоцыганство стали серьезной угрозой. Киберпреступники используют разнообразные методы и техники, чтобы обманным путем получить доступ к нашим личным данным, финансам и даже нарушить нашу репутацию. В данной проектно-исследовательской работе мы предлагаем проанализировать и изучить проблему мошенничества и инфоцыганства в интернете, а также предоставить практические советы и способы борьбы с этими угрозами. Мы будем рассматривать различные аспекты киберпреступлений и исследовать современные технологии и методы защиты, чтобы помочь людям быть более информированными и защищенными в онлайн-среде.

Актуальность: Актуальность проблемы мошенничества и инфоцыганства в интернете заключается в повышенной угрозе для безопасности и конфиденциальности пользователей, требуя необходимости эффективных способов защиты и предотвращения таких преступлений.

Цель работы: Цель данной работы - исследовать проблему мошенничества и инфоцыганства в интернете и предложить эффективные способы борьбы с этими угрозами.

Задачи:

 1. Изучить характеристики и виды мошенничества и инфоцыганства в интернете.

2. Исследовать современные методы обнаружения и предотвращения мошеннических действий в сети.

3. Предложить практические рекомендации для защиты от мошенничества в онлайн-среде.

Предмет: Киберпреступность

Объект: Интернет

Методы исследования:

1. Анализ данных.

2. Изучение реальных случаев.

3. Обзор существующих методов и технологий по борьбе с кибер-преступностью.

Научная новизна: Научная новизна данной работы заключается в представлении современных методов и рекомендаций по борьбе с мошенничеством и инфоцыганством в интернете, основанных на актуальных исследованиях и передовых технологиях.

Теоретическая значимость: Теоретические аспекты в данной работе могут помочь людям безопасно чувствовать себя в интернете.

Практическая значимость: Практическая значимость данной работы заключается в предоставлении конкретных рекомендаций и методов для защиты пользователей от мошенничества и инфоцыганства в интернете, способствуя обеспечению их безопасности в онлайн-среде.

ГЛАВА 1

1.1 Современные виды онлайн-мошенничества

Современные виды онлайн-мошенничества включают:

1. Фишинг: злоумышленники отправляют поддельные электронные письма или создают фальшивые веб-сайты, имитируя легитимные организации, с целью получить личные данные пользователей, такие как пароли, банковские реквизиты или номера социального страхования.

2. Распространение вредоносного ПО: злоумышленники создают вредоносные программы, такие как вирусы, черви или троянские программы, которые могут нанести ущерб компьютерам и украсть конфиденциальную информацию.

3. Инфоцыганство: особая форма киберпреступности, которая предполагает использование информационных технологий для мошеннических действий, включая кражу личных данных, фишинг, создание и распространение вредоносного программного обеспечения и другие виды кибер-атак. Инфоцыгане злоумышленники, которые используют технические средства и методы для незаконного обогащения, они могут злоупотреблять своими знаниями в области информационной безопасности, чтобы обмануть и украсть чужие средства. Есть множество примеров бизнес курсов, тренингов, мошенничество с использованием криптовалют: злоумышленники могут обманывать людей, предлагая фальшивые инвестиционные схемы в области криптовалюты или кражу цифровых кошельков. Мошенничество на онлайн-рынках включает обман при онлайн-покупках или продаже товаров, подделку продуктов и неправомерное использование платежных систем.

Особо опасно инфоцыганство тем, что в первую очередь человек заставляет жертву поверить и доверять ему. Многие блогеры, которых пользуются большой популярностью у молодого поколения в один момент начинают рекламировать и продвигать свои платные курсы по заработку, по изучению криптовалюты, с целью научить человека быстро и легко разбираться в этом и начать зарабатывать. Блогеры-инфоцигане могут представлять себя специалистами в определенной области или использовать обманчивые заголовки и кликбейт для привлечения внимания к своему контенту. Их действия могут вносить путаницу и вводить людей в заблуждение, оказывая влияние на общественное мнение и пользуясь доверием и подписчиками.

1.2 Изучение реальных случаев

Причины, по которым известные люди могут заниматься инфоциганством, могут быть различными. Некоторые из этих причин могут включать желание привлечь больше внимания или получить выгоду за счет создания контента, который вызывает широкую реакцию и споры. Другие могут использовать инфоциганство для повышения своей популярности или привлечения большего количества подписчиков, что может привести к увеличению доходов и инфлюенсерства. Некоторые люди также могут использовать инфоциганство в целях манипулирования общественным мнением или достижения своих политических или личных целей. В целом, причины могут быть разнообразными и зависят от конкретного человека и его мотиваций.

Оксана Самойлова: Супруга рэпера Джигана, модель и бизнес-вумен. Собственный курс успеха продает и жена рэпера Джигана Оксана Самойлова. В своей «Стратегии на миллион» она рассказывает про «тайные знания успешных людей», о «признаках бедности» и дает список «хороших привычек», в который входят, например, такие: «читать аффирмации, принимать витамины, заботиться о своем теле». Ее курсы стоят от 5 тыс. до 300 тыс. рублей.

Виктория Боня: Фотомодель и бывшая звезда «Дома-2» Виктория Боня продает в интернете курс «Я — женщина-богиня», в котором тоже рассказывает женщинам, как «раскрыть силу», впуская в жизнь изобилие и счастье. Во время марафона Боня предлагает участникам, например, практиковать медитацию, в рамках которой нужно дышать пальцами.

Яна Рудковская: Марафон телеведущей, жены Евгения Плющенко и продюсера певца Димы Билана Яны Рудковской «ЯСУПЕР» расскажет, что в маленькой зарплате виновато не государство или обстоятельства, а только вы сами. За 9 тыс. рублей она обещает трансформацию, а также советы по похудению, уходу за собой и почему-то декору. Обещает также дать доступ в закрытый телеграм-канал, в который пишет сама.

Ранее Znak.com писал, что в Думу уже обратились несколько человек, которых обманули недобросовестные блогеры.

«Люди доверчивые, заключали договоры на бизнес-тренинги, не получали желаемого результата, а сейчас считают себя обманутыми. Эта сфера, к сожалению, никак не контролируется государством, поэтому надо ее регулировать. Направим запросы в СКР, МВД, ФНС, чтобы деятельность таких блогеров проверили», — заявил депутат «Справедливой России — За Правду» Сергей Кабыш

ГЛАВА 2

2.1 Обзор существующих методов и технологий по борьбе с кибер-преступностью.

Обзор существующих методов и технологий по борьбе с инфоциганством и мошенничеством в интернете включает следующие подходы:

1. Алгоритмический анализ: использование алгоритмов и аналитических методов для обнаружения и классификации подозрительных активностей, фейковых аккаунтов или распространения дезинформации.

2. Машинное обучение: применение методов машинного обучения и искусственного интеллекта для автоматического обнаружения и фильтрации информации, а также выявления нежелательных действий и поведения.

3. Контроль и модерация платформ: разработка и применение строгих правил и политик модерации на платформах социальных сетей и медиа, чтобы предотвращать и удалять контент, нарушающий правила или содержащий дезинформацию.

4. Образование и осведомленность: проведение образовательных программ и кампаний, чтобы обучить пользователей различать факты от дезинформации и быть более бдительными в отношении подозрительной информации.

5. Международное сотрудничество и законодательство: сотрудничество между правительствами и международными организациями для разработки и применения законодательных мер и политик, направленных на борьбу с мошенничеством и инфоциганством в интернете.

Комбинация этих методов и технологий может помочь в предотвращении и обнаружении мошенничества и инфоциганства, ограничивая их влияние и повышая безопасность пользователей в онлайн-среде.

Чтобы минимизировать возможность попасть на инфоцигана в интернете, вот несколько рекомендаций:

1. Будьте бдительны и критически оценивайте информацию: проверяйте источник информации, особенно если она кажется непроверенной или вызывает сомнения. Используйте достоверные источники новостей и проверенные организации.

2. Поддерживайте конфиденциальность и безопасность своих личных данных: не предоставляйте личную информацию незнакомым или подозрительным лицам в интернете. Будьте осторожны с раскрытием своих личных данных на публичных форумах или социальных сетях.

3. Используйте надежные и обеспеченные платформы: при осуществлении онлайн-транзакций или обработке чувствительных данных используйте только надежные и безопасные интернет-платформы. Проверяйте наличие SSL-сертификатов и прочих мер безопасности соединения.

4. Будьте осторожны с фишинговыми атаками: будьте внимательны к электронным письмам или сообщениям, запрашивающим личную информацию или финансовые данные. Никогда не предоставляйте персональную информацию через непроверенные источники и не переходите по подозрительным ссылкам.

5. Установите антивирусное программное обеспечение и обновляйте его регулярно: имейте на компьютере или мобильном устройстве надежное антивирусное программное обеспечение и следите за обновлениями, чтобы защититься от вредоносных программ и атак.

6. Обращайтесь за помощью и советами: если у вас есть сомнения относительно информации, аккаунтов или сделок в интернете, лучше проконсультироваться с доверенными источниками или экспертами.

Вышеуказанные меры помогут повысить вашу безопасность в онлайн-среде и снизить возможность стать жертвой инфоцигана. Однако, всегда помните, что бдительность и усмотрение являются ключевыми аспектами при использовании интернета.

ЗАКЛЮЧЕНИЕ

В данной проектно-исследовательской работе мы рассмотрели проблему инфоциганства в интернете и рассмотрели различные методы борьбы с ним. Мы изучили характеристики и методы мошенничества, включая фишинг, распространение вредоносного ПО и медиа-инфоциганство. Также мы провели обзор существующих методов и технологий, которые используются для предотвращения и обнаружения таких преступлений.

Наши исследования показали, что проблема инфоциганства все более актуальна в нашей цифровой среде и требует серьезного внимания. Однако существуют эффективные способы борьбы с этими угрозами. Алгоритмический анализ, машинное обучение и модерация платформ являются эффективными инструментами для выявления подозрительной активности и фильтрации контента. Образование и повышение осведомленности пользователей также играют важную роль в защите от инфоциганства.

В заключение, для достижения более безопасной онлайн-среды, взаимодействие между пользователями, организациями и правительственными инстанциями является важным фактором. Безопасность в интернете должна быть приоритетом, и каждый из нас должен быть более бдительным и осведомленным о возможных угрозах. Только так мы сможем преодолеть инфоциганство и создать более доверительную и надежную онлайн-среду для всех.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Цифровые платформы: YouTube, Twich, Facebook, Twitter, Вконтакте, Одноклассники, Yappi, Tik-Tok, Google, Яндекс, Opera.
2. Сайты: compromat.ru, thegirl.ru, dzen.ru, pikabu.ru, glager.ru