Кузнецов Вадим Евгеньевич, курсант,
Московский университет МВД России имени В. Я. Кикотя,
г. Москва

Хмирова Елена Аркадьевна,
старший преподаватель, кафедры иностранных языков,
Московский университет МВД России имени В. Я. Кикотя,
г. Москва

СПОСОБЫ ЗАЩИТЫ ОТ ИНТЕРНЕТ-МОШЕННИЧЕСТВА В РОССИИ И НЕКОТОРЫХ АНГЛОЯЗЫЧНЫХ СТРАНАХ

Аннотация: В современном информационном обществе интернет-мошенничество стало серьезной проблемой, с которой сталкиваются пользователи во всем мире. Интернет-мошенничество представляет собой преступную деятельность, осуществляемую через сеть «Интернет» с целью незаконного получения финансовой выгоды или личной информации путем обмана, манипуляции и злоупотребления доверием пользователей.

Ключевые слова: интернет; мошенничество; фишинг; маркетинг; защита; вредоносные программы;

В данной статье мы рассмотрим различные способы защиты от интернет-мошенничества, как в России, так и в англоязычных странах, и предложим рекомендации по предотвращению мошеннических действий и защите пользователей в сети Интернет. Масштабы интернет-мошенничества растут, и оно оказывает серьезное влияние на финансовую безопасность и неприкосновенность частной жизни пользователей.

Целью данной статьи является исследование способов защиты от интернет-мошенничества в России и некоторых англоязычных странах. Мы стремим-

ся проанализировать различные методы и подходы к борьбе с этой проблемой, а также предложить практические рекомендации для защиты пользователей в онлайн-среде.

Актуальность исследования обусловлена необходимостью обеспечения безопасности и защиты интернет-пользователей от мошеннических атак. Результаты нашего исследования могут быть полезными для органов правопорядка, специалистов в области информационной безопасности и пользователей, которым необходимо принять меры для защиты своих личных и финансовых данных в онлайн-среде.

Для того, чтобы проникнуться в тему исследования следует рассмотреть типы интернет-мошенничества. Они включают в себя разнообразные схемы и методы, используемые мошенниками для обмана пользователей и получения незаконной выгоды. Рассмотрим некоторые распространенные типы интернет-мошенничества:

1. Фишинг: Мошенники создают поддельные веб-сайты, электронные письма или сообщения, имитирующие легитимные организации или сервисы, чтобы получить личные данные и финансовую информацию от пользователей.
2. Мошенничество с использованием вредоносных программ: Мошенники разрабатывают и распространяют вредоносное программное обеспечение, такое как вирусы, трояны или рекламные шпионы, с целью получить доступ к компьютерам или украсть личные данные.
3. Кража личных данных: Мошенники пытаются получить доступ к личным данным пользователей, таким как имена, адреса, номера социального страхования или банковские реквизиты, для совершения финансовых мошенничеств или идентификационных краж.
4. Мошенничество при онлайн-покупках: Мошенники предлагают поддельные товары или услуги через интернет, получают предоплату от покупателей, но не поставляют товары или предоставляют некачественные услуги.

Далее следует раскрыть факторы, которые способствуют росту интернет-мошенничества. Некоторые из них включают:

1. Анонимность и конфиденциальность: Интернет предоставляет мошенникам возможность скрывать свою идентичность и оставаться незаметными, что облегчает совершение мошеннических действий.

2. Глобальный охват: Интернет позволяет мошенникам достигать широкой аудитории по всему миру, что увеличивает потенциальное количество жертв.

3. Недостаточная осведомленность пользователей: Некоторые пользователи не имеют достаточного знания о методах интернет-мошенничества и не принимают необходимые меры предосторожности при онлайн-взаимодействиях.

4. Технические уязвимости: Наличие уязвимостей в системах безопасности и программном обеспечении может быть использовано мошенниками для атак и эксплуатации.

Понимая эти факторы, мы сможем лучше ориентироваться в причинах и способах противодействия интернет-мошенничеству.

Существует ряд эффективных мер, которые можно принять для защиты от интернет-мошенничества:

Важно получить образование и информированность о различных видах интернет-мошенничества и их характеристиках. Имеет место постоянное обучение, чтобы понимать риски и быть внимательными к подозрительным ситуациям или запросам.

Рекомендуется использовать сильные, уникальные пароли для каждой учетной записи. Пароли должны быть сложными, содержать комбинацию букв, цифр и специальных символов. Это поможет предотвратить несанкционированный доступ.

Важно регулярно обновлять программное обеспечение на устройствах. Обновления часто включают исправления уязвимостей, что помогает предотвратить атаки мошенников.

Имеет место использование безопасных соединений при передаче конфиденциальной информации или совершении финансовых операций. Рекомендуется использовать защищенные протоколы передачи данных, такие как SSL/TLS, а также подключаться к защищенным Wi-Fi сетям.

Рекомендуется проверять подлинность источника, прежде чем предоставлять личные данные или финансовую информацию. Важно быть осторожным с подозрительными электронными письмами, сообщениями или веб-сайтами, которые могут быть поддельными или запрашивать чувствительные данные.

Следует установить надежное антивирусное программное обеспечение на устройства и регулярно обновлять его. Это поможет обнаруживать и блокировать вредоносные программы или атаки.

Не менее важно быть бдительным при совершении онлайн-покупок. Рекомендуется проверять репутацию продавца, читать отзывы других покупателей и использовать надежные платежные системы.

Имеет место регулярная проверка банковских и финансовых отчетов на наличие подозрительных операций или несанкционированных транзакций. В случае обнаружения подозрительных действий рекомендуется немедленно сообщить об этом банку или провайдеру платежей.

Это лишь несколько способов защиты от интернет-мошенничества. Важно понимать, что защита требует постоянного внимания и активной реакции со стороны пользователей.

О важности защиты говорит и тот факт, что в современном мире происходило множество инцидентов, связанных с кражей данных пользователей. Одной из таких ситуаций был инцидент с компанией Equifax, одним из трех крупнейших американских агентств кредитной истории. В 2017 году был обнародован случай крупномасштабной кибератаки, в результате которой хакеры полу-

чили доступ к личным данным более 143 миллионов американских граждан, включая их имена, социальные страховые номера, даты рождения, адреса и номера водительских удостоверений. Кража персональных данных на таком масштабе вызвала серьезное беспокойство и негодование общественности.

Этот случай стал ярким примером того, как уязвимости в системах защиты данных могут привести к серьезным последствиям и негативным последствиям для множества людей. Он подчеркивает важность постоянного обновления и улучшения мер безопасности, а также повышение осведомленности о рисках и методах защиты персональных данных в цифровой среде.

В России и англоязычных странах проблема интернет-мошенничества проблема кражи данных широко распространена и требует принятия мер для эффективной защиты. Одной из основных стратегий является укрепление сотрудничества между правоохранительными органами и интернет-провайдерами. Это позволит обменять информацией о новых методах мошенничества, быстро реагировать на инциденты и предпринимать совместные действия по выявлению и привлечению виновных лиц к ответственности.

Также необходимо повышать осведомленность об интернет-мошенничестве среди населения. Это можно осуществлять через проведение информационных кампаний, обучающих семинаров и распространение информации о типичных схемах мошенничества. Пользователи должны быть предупреждены о возможных угрозах и научены распознавать подозрительные ситуации, чтобы предотвратить попадание в ловушку мошенников. Для более эффективной борьбы с интернет-мошенничеством могут быть рассмотрены следующие идеи и решения:

Продолжение разработки и внедрение инновационных технологических решений, таких как системы идентификации пользователей, многофакторная аутентификация и технологии блокчейн. Эти механизмы могут обеспечить дополнительный уровень безопасности и защиты при совершении онлайн-транзакций или передаче конфиденциальных данных. Важно развивать между-

народное сотрудничество в области борьбы с интернет-мошенничеством. Обмен информацией и опытом с другими странами позволит эффективнее выявлять и пресекать глобальные мошеннические схемы и сотрудничать в проведении расследований и привлечении преступников к ответственности. Внедрение строгих регулятивных мер, включая законодательные нормы и наказания, для пресечения интернет-мошенничества, позволит включать санкции против мошенников, ужесточение требований к защите данных и обязательную сертификацию для интернет-провайдеров и платежных систем. Все эти меры должны приниматься совместно государственными органами, правоохранительными структурами, интернет-провайдерами и самими пользователями, чтобы эффективно бороться с интернет-мошенничеством и обеспечить безопасность онлайн-среды.

Таким образом, на основе проведенного анализа мы можем сделать следующие основные выводы:

Интернет-мошенничество представляет серьезную угрозу как в России, так и в англоязычных странах. Оно наносит значительный ущерб как отдельным лицам, так и бизнесу, а также подрывает доверие к онлайн-платформам и электронным транзакциям.

Защита от интернет-мошенничества требует комплексного подхода, включающего образование пользователей, применение технических мер безопасности, регулятивные меры и сотрудничество на международном уровне.

Принятые меры по защите от интернет-мошенничества имеют определенную эффективность, но требуют постоянного анализа и усовершенствования. Технологические инновации и международное сотрудничество играют важную роль в повышении эффективности защиты.

Однако, интернет-мошенничество постоянно эволюционирует, поэтому дальнейшие исследования и разработки в области защиты необходимы. Необходимо постоянно изучать новые методы мошенничества и адаптировать меры защиты к новым вызовам.

Значимость дальнейших исследований и разработок в области защиты от интернет-мошенничества несомненна. Продолжение исследований поможет улучшить понимание механизмов мошенничества, разработать новые технические решения и подготовить эффективные стратегии борьбы с мошенниками.

В заключение, защита от интернет-мошенничества остается актуальной и важной задачей. Коллективные усилия, включая осведомленность пользователей, сотрудничество между государствами и разработку инновационных решений, позволят снизить уровень интернет-мошенничества и обеспечить безопасность в онлайн-среде.

Список литературы:

1. Атаева Г.И. Информационные технологии и современное образование // Молодой учёный. № 10, 2016. С. 1166-1167.
2. Белоножко Е.С., Чеджемов Г.А. Мошенничество в сети Интернет // Наука XXI века: актуальные направления развития. Самара. СГЭУ. – 2017. – №1-1. – С. 86.
3. Официальный сайт компании «Лаборатория Касперского». – [Электронный ресурс]. – Режим доступа: http://www.kaspersky.ru
4. Шейнов, В. П. Как защититься от обмана и мошенничества: моногр. // В.П. Шейнов. – М.: Харвест, 2019. – 464 с.