Научная статья
https://doi.org/:10.29039/2312-7937-2025-2-125-129
EDN: https://elibrary.ru/fewfjm

Карданов Руслан Рейзаевич
кандидат юридических наук
Северо-Кавказский институт повышения квалификации (филиал)
Краснодарского университета МВД России
(Нальчик, КБР, Россия)
ruslan-nalchik@yandex.ru

Рясов Александр Алексеевич
кандидат юридических наук, доцент
Ставропольский филиал Краснодарского университета МВД России
(Ставрополь, Россия)
identifiks@mail.ru

К ВОПРОСУ О ПРОТИВОДЕЙСТВИИ ФИШИНГОВЫМ АТАКАМ

Аннотация. *Статья исследует проблему фишинга - широко распространенной формы кибермошенничества, основной целью которого является получение конфиденциальной информации пользователей путем их обмана. Фишинг включает создание поддельных веб-сайтов и рассылку фальшивых писем, замаскированных под официальные сообщения. Статья касается истории развития фишинга, подчеркивая, что с увеличением числа пользователей интернета и внедрением новых технологий этот вид мошенничества стал более изощренным и массовым.*

В статье выделяется несколько методов фишинга, включая использование электронной почты, мобильных устройств, персонализацию атак и создание клонов популярных сайтов. Особое внимание уделяется социальным приемам, используемым мошенниками для манипуляции жертвами, таким как игра на человеческих эмоциях и доверии. Современные достижения в области нейронных сетей и чат-ботов, таких как ChatGPT, создают дополнительные риски, позволяя мошенникам делать свои письма еще более реалистичными.

Особое внимание уделяется причинам высокой эффективности фишинговых схем, включая психологическое давление, внезапные соблазнительные предложения и использование страха перед потерей данных или средств. Статья также затрагивает вопрос о роли социальной инженерии в кибератаках и предлагает меры по повышению уровня киберграмотности среди пользователей.

Статья акцентирует внимание на серьезных последствиях фишинга, которые включают потерю средств, персональные данные и доступ к важным учетным записям. Подчеркивается необходимость повышения уровня осведомленности и разработки эффективных мер защиты против фишинговых атак.

Ключевые слова: *фишинг, смэшинг, вишинг, кибербезопасность, социальная инженерия, конфиденциальные данные, поддельные сайты, фальшивые письма, фильтрация почты, многоуровневая аутентификация*

Для цитирования: *Карданов Р.Р., Рясов А.А. К вопросу о противодействии фишинговым атакам // Вестник ВИПК МВД России. 2025. № 2(74). С. 125-129; https://doi.org/:10.29039/2312-7937-2025-2-125-129.*

KARDANOV RUSLAN R.
North Caucasian Institute for Advanced Studies (branch) Krasnodar University
of the Ministry of Internal Affairs of Russia (Nalchik, KBR, Russia)

RYASOV ALEXANDER A.
PhD, associate professor
Stavropol branch of the Krasnodar University of the Ministry of Internal Affairs of Russia
(Stavropol, Russia)

ON THE ISSUE OF COUNTERING PHISHING ATTACKS

Abstract. *The article examines the problem of phishing, a widespread form of cyber fraud, the main purpose of which is to obtain confidential information from users by deceiving them. Phishing involves creating fake websites and sending fake emails disguised as official messages. The article describes the history of phishing, emphasizing that with the increase in the number of Internet users and the introduction of new technologies, this type of fraud has become more sophisticated and widespread.*

The article highlights several phishing methods, including the use of email, mobile devices, personalization of attacks, and the creation of clones of popular sites. Particular attention is paid to social techniques used by scammers to manipulate victims, such as playing on human emotions and trust. Modern advances in neural networks and chatbots, such as ChatGPT, create additional risks, allowing scammers to make their letters even more realistic.

Particular attention is paid to the reasons for the high effectiveness of phishing schemes, including psychological pressure, sudden tempting offers, and the use of fear of losing data or funds. The article also touches upon the role of social engineering in cyberattacks and suggests measures to increase cyber literacy among users. The article focuses on the serious consequences of phishing, which include loss of funds, personal data, and access to important accounts. The author emphasizes the need to raise awareness and develop effective measures to protect against phishing attacks.

Keywords: *phishing, smashing, vishing, cybersecurity, social engineering, sensitive data, fake websites, fake emails, mail filtering, multi-level authentication*

For citation: *Kardanov R.R., Ryasov A.A. On the issue of countering phishing attacks // Vestnik Advanced Training Institute of the MIA of Russia. 2025. № 2(74). P. 125-129 ; https://doi.org/:10.29039/2312-7937-2025-2-125-129.*

Вступительная часть.

Фишинг представляет собой одну из наиболее распространённых и коварных форм мошенничества в сфере компьютерной информации, цель которых заключается в обмане пользователей с целью кражи их конфиденциальной информации, такой как пароли, номера кредитных карт и другая чувствительная информация. При совершении таких преступлений «преступники перенаправляют пользователей на поддельные сетевые ресурсы, которые создаются заранее. Простым пользователям неподлинные интернет-ресурсы сложно отличить от подлинных, и поэтому, осуществляя переход на них по прикрепленным к полученным на электронную почту письмам-ссылкам, пользователи попадают на поддельные сайты злоумышленников» [1, с. 246]. В последние годы фишинг стал одной из самых серьёзных угроз в сфере кибербезопасности, оказывая значительное влияние на частные лица, организации и правительства, как в России, так и по всему миру. «Количество фишинговых атак в России увеличилось на 425% в 2024 году. За тот же период было заблокировано свыше 22 тысяч фишинговых сайтов, как сообщил руководитель Центра мониторинга и управления сетью связи общего пользования (ЦМУ ССОП), подведомственного Роскомнадзору, Сергей Хуторцев» [2].

Актуальность этой темы обусловлена несколькими факторами. Во-первых, фишинговая деятельность непрерывно развивается, становясь всё более сложной и изощренной. Современные фишеры используют продвинутые технологии социальной инженерии, мимикрию под легитимные сайты и услуги, а также внедряются в цепочки поставок программного обеспечения, чтобы заманить жертв в ловушку. Во-вторых, рост популярности удалённой работы и цифрового взаимодействия сделал людей ещё более уязвимыми к подобным атакам. Наконец, фишинг остаётся одним из наиболее прибыльных типов киберпреступлений, что стимулирует его дальнейшее развитие.

Основная часть.

Фишинг опасен своей скрытностью и убедительностью. Часто жертвы даже не осознают, что стали объектом мошенничества, пока не столкнутся с последствиями – потерянными деньгами, украденными личными данными или взломанными аккаунтами.

Популяризация ChatGPT предоставляет преступникам возможность создавать высококачественные тексты и структуры сообщений, даже если целевая аудитория находится в другой языковой среде. Раньше распознавание фишинговых писем могло основываться на обнаружении грамматических ошибок, стилистических неточностей или странного тона текста, но теперь использование

нейросетей сводит такие ошибки к минимуму, делая атаки более эффективными [3, с. 113-118].

На начальном этапе становления фишинга мошеннические схемы базировались на системах мгновенного обмена сообщениями, нацеливаясь на убеждение жертвы в необходимости предоставления конфиденциальных данных, которые затем использовались для массовой рассылки нежелательного контента. Основными мишенями в тот период выступали обычные пользователи, так как далеко не каждый имел доступ к банковским услугам. Однако стремительное развитие цифровых финансовых экосистем и сопутствующих информационных технологий привело к изменению ситуации. Сегодня в группе повышенного риска оказываются не только физические лица, но и их материальные активы, учитывая широкое распространение банковских счетов, кредитных и дебетовых карт. В результате наблюдается рост объемов электронных платежей, что влечет за собой увеличение численности фишеров и расширение масштабов совершаемых ими преступлений. Данная тенденция делает проблему фишинга одной из ключевых угроз современного информационного общества.

Фишеры действуют, манипулируя человеческими эмоциями. Они не прибегают к прямому насилию, предпочитая действовать хитроумно, добиваясь доверия жертвы. Это требует высокой квалификации и опыта, что усложняет расследование таких преступлений.

Зачастую фишеры, помимо технологических средств, активно используют человеческие слабости и доверие такие как: сексуальное влечение, жадность, тщеславие, чрезмерная доверчивость, лень, сострадание и поспешность в принятии решений.

К основным способам совершения фишинговых атак можно отнести следующие:

1. Мошенничество с электронной почтой. Это разновидность мошенничества, когда преступник притворяется поставщиком или бизнес-партнером и уговаривает сотрудника компании перевести значительную сумму денег на офшорный счет, выдавая это за оплату услуг, которые фактически не были оказаны.

2. Фишинг с использованием сервиса Google Календарь. Этот метод заключается в массовой рассылке мошеннических сообщений жертвам, маскируя их под автоматические уведомления в календаре смартфона. Данный подход представляет собой новую форму фишинговых атак, которая имеет потенциал обмануть даже опытных пользователей, знакомых с угрозой спама и фишинга в электронной почте и мессенджерах.

Злоумышленники используют функцию автоматического добавления событий в календарь и отправки уведомлений об этих событиях. Поскольку у большинства пользователей данная функция активирована по умолчанию, сообщение, имитирующее официальное уведомление от приложений Google Calendar, может легко ввести жертву в заблуждение. Открыв всплывающее окно на смартфоне, пользователь видит ссылку на фишинговый сайт, где предлагается пройти простой опрос за вознаграждение. Чтобы получить приз, пользователю предлагают оплатить небольшую комиссию, введя данные банковской карты и личные сведения, такие как имя, телефон и адрес. Эти данные попадают прямо в руки злоумышленников.

3. Смэшинг — это вид мошенничества, аналогичный фишингу, но осуществляемый через SMS-сообщения. Вместо отправки электронных писем злоумышленники отправляют своим жертвам текстовые сообщения, предназначенные для обмана и получения конфиденциальной информации, такой как PIN-коды для доступа к онлайн-банкингу. Некоторые смэшинговые сообщения могут перенаправлять пользователей на поддельные веб-сайты или предлагать загрузить вредоносные приложения, замаскированные под полезные программы. При этом практически все смэшинговые сообщения содержат элемент срочности. Например, вам могут сказать, что ваш банковский аккаунт был взломан, и настоятельно рекомендуют немедленно перейти по ссылке для восстановления доступа.

4. Целевой фишинг. Заключается в отправке персонализированных писем определённым лицам, представляющим интерес для мошенников. В отличие от массовых рассылок, целевой фишинг направлен на конкретных сотрудников в заранее отобранных организациях. Эти письма отличаются высокой степенью

персонализации, создавая у жертвы ощущение, будто она знакома с отправителем, что усиливает доверие и увеличивает вероятность успеха атаки. Чаще всего мишенями становятся топ-менеджеры и руководители крупных компаний. Возможно даже использование нейросетей с целью изменения внешности или голоса звонящего. После компрометации аккаунта высокопоставленного сотрудника, от его имени могут поступать распоряжения подчинённым, такие как переводы средств, оплата несуществующих услуг или передача личных данных.

5. Вишинг - это разновидность мошенничества, при которой злоумышленники используют телефонные звонки для получения конфиденциальной информации от жертв, часто применяя методы социальной инженерии.

Как правило, вишинг начинается с звонка, во время которого мошенник может представляться работником банка, службы безопасности или другой авторитетной организации. Сценарий часто включает в себя автоматическое голосовое сообщение или личный разговор, в ходе которого жертве сообщают о подозрительной активности на ее счете или необходимости подтверждения данных.

Злоумышленники могут использовать частично известную информацию о жертве, например, имя, фамилию или номер банковской карты, что создаёт иллюзию доверия. После этого они могут запросить подтверждение личности, например, спрашивая секретный код, который приходит в SMS, или другие идентификационные данные [4, с. 280].

В случае, если жертва с ними сотрудничает и предоставляет необходимую информацию, мошенники могут получить доступ к банковскому счету или другим финансовым ресурсам, что приводит к потере средств.

6. Клон-фишинг - это метод, при котором мошенники дублируют ранее полученные жертвой законные письма от легитимного отправителя. Затем они вносят незначительные изменения, заменяя контакты или ссылки на поддельные, что приводит к утечке конфиденциальной информации при взаимодействии с такими подложными элементами.

7. Метод «Wi-Fi двойник» подразумевает создание точной копии легального беспроводного соединения, которая заманивает ничего не подозревающих пользователей на фишинговый сайт. После подключения к такой сети жертвы часто сталкиваются с просьбой ввести свои личные данные, например логины и пароли, которые сразу же оказываются в руках злоумышленников. Получив эту информацию, хакеры могут получить доступ к сетевым ресурсам, перехватывать незашифрованные данные и использовать их для дальнейшего проникновения и кражи конфиденциальных сведений.

8. Поисковый фишинг заключается в создании хакерами собственных веб-сайтов, которые затем индексируются в обычных поисковых системах. Эти сайты обычно предлагают слишком заманчивые предложения и дешёвые товары, чтобы привлечь ничего не подозревающих покупателей, которые находят такие страницы в результатах поиска Google или других поисковиков. Когда жертва переходит по ссылке на такой сайт, её просят зарегистрироваться или ввести платёжные реквизиты для завершения покупки. Таким образом, мошенники получают доступ к личным данным, которые позже используются для кражи финансов.

Среди тем, которые более всего используют фишеры для совершения мошеннических действий, можно выделить следующие:

рабочая почта. Тематика корпоративных рассылок становится все более популярной среди мошенников, особенно если речь идет о письмах, касающихся изменения заработной платы, условий социального обеспечения или тарифов на банковские услуги;

новые фильмы и сериалы. В преддверии громких кинопремьер злоумышленники создают копии сайтов популярных стриминговых платформ, чтобы завладеть платежными реквизитами и данными аккаунтов;

финансовые уловки. Мошенники выдают себя за крупные банки и финансовые организации, обещая бонусные программы, скидки на кредиты или компенсацию потерь от прошлых махинаций, а также предупреждают о мнимых неполадках в мобильных приложениях банка;

туризм и отдых. Фейковые предложения по бронированию отелей и авиабилетов по привлекательным ценам – классический

прием для привлечения жертв через фишинговые сайты и письма;

онлайн-знакомства. Желание завести новые отношения используется мошенниками для создания фиктивных профилей и назначения встреч, после которых потерпевшие лишаются как денег, так и личных данных;

платежи за подписки. Пользователи получают письма с предложениями обновить или оформить подписку на различные цифровые сервисы, причем эти сообщения кажутся вполне правдоподобными;

инвестиционные схемы. В условиях роста интереса к вложениям в криптовалюты, нефть и газ, злоумышленники создают липовые площадки, мимикрирующие под реальные инвестиционные проекты, и собирают средства с доверчивых инвесторов.

Чтобы распознать фишинговые письма и сайты, следует обращать внимание на следующие признаки:

1. Общие или неофициальные приветствия. Если отправитель не обращается к получателю письма по имени, а использует обращения типа «дорогой друг» или «уважаемый клиент».

2. Неожиданно привлекательные предложения. Мошенники часто обещают лёгкий заработок, дорогие призы за участие в опросах или компенсации за просмотр рекламы.

3. Подозрительные домены. Настоящие компании обычно используют домены, совпадающие с их названием. Если название сайта не соответствует названию компании, это повод насторожиться.

4. Угрозы и запугивание. Мошенники могут пытаться вызвать панику, угрожая блокировкой аккаунта или юридическими последствиями, если получатель письма не предпримет немедленных действий.

5. Призывы к спешке. Спешка — частый признак мошенничества.

6. Запросы личной информации (фотографии документов или данные банковских карт).

7. Ошибки и небрежности в оформлении сообщений. Многочисленные ошибки, лишние пробелы, странные замены букв могут указывать на то, что сообщение создано с целью обхода антиспам-защиты или что его авторы недостаточно компетентны в русском языке.

Эти рекомендации помогут распознавать большинство фишинговых атак, однако следует помнить, что некоторые профессиональные мошенники способны создавать почти идеальные письма и сайты.

Заключительная часть.

Исходя из этого, можно заключить, что наряду с правовыми механизмами противодействия фишингу, ключевую роль играет осведомлённость самих пользователей. Большинство фишинговых атак можно предотвратить, соблюдая элементарные правила безопасности. Пользователям рекомендуется внимательно проверять источники сообщений, обращать внимание на подлинность сайтов и ссылок. Организации также вносят вклад в борьбу с фишингом, предупреждая клиентов о возможных угрозах и предоставляя доказательства аутентичности своих ресурсов. Важным фактором снижения уровня ущерба от фишинга является просвещение населения о правилах безопасного поведения в интернете, включая использование электронных платёжных систем.

Одним из важнейших подходов в борьбе с фишинговыми атаками является использование технологий интеллектуального машинного обучения. Эти технологии встраиваются в браузеры и формируют систему классификации, которая позволяет выявлять хакерские атаки и немедленно информировать пользователей о возможной опасности.

Список источников

1. Коровин И. К., Щербина М. А. Способы совершения мошенничества в сети Интернет как элементы криминалистической характеристики // Лучшая научная статья 2018: сб. статей XVII Международного науч.-исследовательского конкурса (г. Пенза, 30 мая 2018 г.). - Пенза: МЦНС «Наука и Просвещение», 2018.
2. ТАСС: сайт // URL: https://tass.ru/obschestvo/22215161.
3. Курин А.А., Карданов Р.Р., Евстифеева Е.П. Направления развития системы информационно-аналитического обеспечения раскрытия и расследования преступлений // Право и управление. 2022. № 8.
4. Колиев В.В. Тактика и методика расследования преступлений, совершаемых с помощью сети Интернет // Право и государство: теория и практика. 2021. № 4 (196).

Информация об авторах:

Р.Р. Карданов, *старший преподаватель кафедры деятельности ОВД в особых условиях*

А.А. Рясов, *профессор кафедры уголовного процесса и криминалистики*

About the authors:

R.R. Kardanov, *Senior Lecturer, Department of Activities of the Internal Affairs Directorate in Special Conditions*

A.A. Ryasov, Professor of the Department of Criminal Procedure and Forensic Science

Статья поступила в редакцию 27.03.2025