Нижлукченко И.Д. Фишинговые атаки и как их распознать: анализ наиболее распространенных методик фишинга и советы по их идентификации и предотвращению // Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 5(43) с. 98–103

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ФИШИНГОВЫЕ АТАКИ И КАК ИХ РАСПОЗНАТЬ: АНАЛИЗ НАИБОЛЕЕ РАСПРОСТРАНЕННЫХ МЕТОДИК ФИШИНГА И СОВЕТЫ ПО ИХ ИДЕНТИФИКАЦИИ И ПРЕДОТВРАЩЕНИЮ

Нижлукченко И.Д.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: nizhluchenk@gmail.com

Эта статья представляет собой всесторонний анализ фишинговых атак, их специфики, наиболее распространенных методик, а также стратегий для их идентификации и предотвращения. Освещая тему с различных аспектов, статья детально рассматривает механизмы, с помощью которых злоумышленники осуществляют атаки, предоставляя читателю глубокое понимание того, как фишинговые сообщения создаются и распространяются через электронную почту, социальные сети, SMS и другие цифровые каналы. Помимо этого, в статье предлагаются практические советы по обеспечению кибербезопасности, включая использование технических средств защиты и образовательных программ для снижения риска фишинговых атак. Анализируется важность анализа и отчетности в борьбе против киберпреступности, подчеркивая значимость совместных усилий в обмене информацией и разработке стратегий защиты.

Ключевые слова: Фишинг, кибербезопасность, идентификация фишинга, предотвращение фишинга, методики фишинга, анализ фишинговых атак, защита от фишинга, образование в области кибербезопасности.

PHISHING ATTACKS AND HOW TO RECOGNIZE THEM: AN ANALYSIS OF THE MOST COMMON PHISHING TECHNIQUES AND TIPS FOR IDENTIFYING AND PREVENTING THEM

Nizhlukchenko I.D.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: nizhluchenk@gmail.com

This article provides a comprehensive analysis of phishing attacks, their specifics, the most common techniques, as well as strategies for their identification and prevention. Covering the topic from various aspects, the article examines in detail the mechanisms by which attackers carry out attacks, providing the reader with a deep understanding of how phishing messages are created and distributed through email, social networks, SMS and other digital channels. In addition, the article offers practical tips on ensuring cybersecurity, including the use of technical means of protection and educational programs to reduce the risk of phishing attacks. The importance of analysis and reporting in the fight against cybercrime is analyzed, emphasizing the importance of joint efforts in the exchange of information and the development of protection strategies.

Keywords: Phishing, cybersecurity, phishing identification, phishing prevention, phishing techniques, phishing attack analysis, phishing protection, cybersecurity education.

В последние десятилетия интернет стал неотъемлемой частью нашей повседневной жизни. Этот цифровой мир предоставил невероятные возможности для обучения, ведения бизнеса и общения. Однако, вместе с прогрессом пришли и новые угрозы, одной из которых являются фишинговые атаки. Фишинг — это тип кибератаки, цель которой заключается в том, чтобы обманом заставить жертву раскрыть конфиденциальную информацию, такую как пароли, данные кредитных карт и банковские сведения. Эта статья направлена на анализ наиболее распространенных методик фишинга, предоставление советов по их идентификации и предотвращению.

Фишинговые атаки часто маскируются под легитимные запросы от известных компаний или социальных сетей. Атакующие используют различные платформы: электронную почту, социальные сети, SMS и веб-сайты. Сообщения могут содержать прямые призывы к действию, такие как подтверждение учетной записи или изменение пароля, и часто сопровождаются ссылками на поддельные веб-сайты, визуально неотличимые от настоящих.

Фишинговые атаки имеют свою уникальную специфику, которая выделяет их среди других видов киберугроз. Эти атаки основаны на манипуляции и обмане, где злоумышленники стараются выдать себя за доверенные лица или организации. Часто фишинговые сообщения выглядят как официальные запросы от известных компаний, банков или социальных сетей, и могут призывать жертву к срочным действиям — например, подтвердить учетную запись или обновить пароль. Эти сообщения могут приходить через различные каналы коммуникации, включая электронную почту, мессенджеры, социальные сети и даже SMS.

Одним из характерных признаков фишинга является использование поддельных веб-сайтов, которые внешне почти не отличаются от настоящих.[3] Злоумышленники тщательно копируют дизайн и структуру реальных сайтов, чтобы убедить пользователя в подлинности своего запроса. При этом, даже минимальное несоответствие в адресе сайта или в его визуальном оформлении может выдать подделку. Особенно это касается случаев, когда для перехода на сайт используются ссылки из сообщений: они могут вести на вредоносные страницы, где пользователь, не подозревая обмана, вводит свои конфиденциальные данные.

Эти атаки опираются на элемент неожиданности и психологическое давление. Зачастую жертвам предлагается немедленно предпринять какие-то действия, чтобы избежать негативных последствий, таких как блокировка аккаунта или потеря средств. Этот метод спешки создает условия, при которых человек менее склонен задумываться о подлинности запроса и больше подвержен риску совершить ошибку. Именно эта специфика делает фишинговые атаки особенно опасными, поскольку они направлены на эксплуатацию человеческого фактора, а не технических уязвимостей системы.

Методики фишинга разнообразны и постоянно эволюционируют, поскольку злоумышленники ищут новые способы обмана пользователей и обхода систем безопасности. В основе фишинга лежит психологический маневр, направленный на вызов доверия или страха, чтобы мотивировать жертву к действию, чаще всего к разглашению конфиденциальной информации. В этом контексте фишинг адаптируется к различным сценариям использования и технологическим платформам, чтобы максимально увеличить свою эффективность.

Одним из основных методов является спир-фишинг, который отличается высокой степенью персонализации. Злоумышленники собирают информацию о своих целях, используя

открытые источники или предыдущие утечки данных, чтобы создать сообщения, кажущиеся максимально достоверными. Эти сообщения могут имитировать переписку от коллег, друзей или руководителей, часто ссылаясь на конкретные детали, знакомые жертве, что делает атаку особенно убедительной.

Вайлинг углубляет концепцию спир-фишинга, нацеливаясь на верхушку иерархической лестницы — высокопоставленных руководителей организаций. В этих случаях сообщения могут содержать запросы на перевод средств или предоставление конфиденциальной корпоративной информации, маскируясь под срочные деловые потребности.

Фарминг, в отличие от других методов, фокусируется на техническом манипулировании, направленном на перенаправление пользователей с легитимных сайтов на поддельные, часто с помощью заражения DNS-серверов или внедрения вредоносного ПО. Этот метод позволяет атакующим перехватывать данные пользователя незаметно для него.

Смишинг и вишинг применяют традиционные каналы связи, такие как SMS и телефонные звонки, для доставки фишинговых сообщений. Эти атаки используют схемы, в которых злоумышленники выдают себя за представителей банков или других уважаемых организаций, убеждая жертву предоставить личную информацию или выполнить финансовые операции под предлогом проверки счета или обновления безопасности.

В целом, разнообразие методик фишинга отражает адаптивность и изобретательность злоумышленников в их стремлении обмануть пользователей. Эффективная защита требует постоянного осведомления о новых методах атак и культуры безопасного поведения в интернете.

Идентификация и предотвращение фишинговых атак требуют комплексного подхода, который включает в себя образование пользователей, использование технических средств безопасности и внедрение строгих процедур обработки информации. Одной из ключевых стратегий является развитие критического мышления и бдительности при работе с электронной почтой и другими цифровыми каналами.[5] Пользователи должны научиться распознавать потенциальные признаки фишинговых сообщений, такие как несоответствие адреса отправителя, наличие орфографических и грамматических ошибок, странное форматирование и необычное использование языка, а также подозрительные призывы к действию.

Обучение и повышение осведомленности среди сотрудников и пользователей играет важную роль в предотвращении фишинга. Регулярные тренинги и симуляции фишинговых атак могут помочь людям лучше понять, как выглядят фишинговые атаки в реальности, и как на них правильно реагировать. Кроме того, важно подчеркнуть необходимость осторожного отношения к личной и корпоративной информации, учить не раскрывать ее без достаточной проверки легитимности запроса.

На техническом уровне, использование современных инструментов безопасности, таких как антивирусное и антифишинговое программное обеспечение, может значительно уменьшить риск успешной фишинговой атаки.[2] Эти инструменты могут автоматически отфильтровывать подозрительные письма, предупреждать пользователей о потенциально опасных сайтах и блокировать доступ к известным вредоносным ресурсам.

Двухфакторная аутентификация представляет собой еще один эффективный способ защиты от последствий фишинговых атак, поскольку даже в случае компрометации логина и

пароля злоумышленникам будет значительно сложнее получить доступ к защищаемым ресурсам без второго фактора аутентификации.

Важной частью стратегии предотвращения фишинга является также разработка и внедрение четких процедур обработки запросов на доступ к информации или выполнение финансовых операций. Это включает в себя требования к двойной проверке и подтверждению таких запросов через альтернативные каналы связи, что значительно усложняет задачу для атакующих.

В совокупности, эти меры формируют многоуровневую систему защиты, которая помогает снизить риск успешных фишинговых атак и минимизировать их потенциальный ущерб.

В борьбе с фишинговыми атаками принятие эффективных мер предосторожности является ключевым элементом защиты как индивидуальных пользователей, так и организаций в целом. Важным шагом в этом направлении является укрепление системы аутентификации пользователей. Внедрение двухфакторной аутентификации значительно увеличивает безопасность, поскольку даже в случае, если злоумышленники сумеют узнать пароль пользователя, дополнительный уровень проверки может предотвратить несанкционированный доступ к учетной записи.

Помимо технических средств, большое значение имеет повышение осведомленности и образовательный аспект. Регулярное обучение сотрудников и пользователей, проведение тренингов по кибербезопасности и симуляции фишинговых атак помогают развивать критическое мышление и учат распознавать потенциальные угрозы.[4] Ведь осознанное отношение к безопасности в интернете и умение идентифицировать подозрительные сообщения и веб-страницы являются мощным инструментом противодействия фишингу.

Кроме того, регулярное резервное копирование данных обеспечивает дополнительный уровень защиты. В случае успешной фишинговой атаки, направленной на кражу или шифрование данных, наличие актуальных копий позволяет быстро восстановить информацию и минимизировать потери.

Использование специализированного программного обеспечения для защиты от фишинга также играет важную роль в обеспечении кибербезопасности. Антивирусные и антифишинговые решения могут автоматически блокировать доступ к известным вредоносным сайтам, анализировать входящие сообщения на предмет подозрительного содержимого и предупреждать пользователей о потенциальных угрозах.

В совокупности, эти меры предосторожности создают многоуровневую защиту, которая охватывает как технические аспекты безопасности, так и человеческий фактор. Внедрение комплексного подхода к кибербезопасности, включающего как передовые технологии, так и постоянное обучение и повышение осведомленности, является наиболее эффективной стратегией противодействия фишинговым атакам.Анализ и отчетность

Анализ и отчетность о фишинговых атаках играют ключевую роль в цикле улучшения кибербезопасности организации. Этот процесс начинается с момента обнаружения подозрительной активности или атаки и включает в себя сбор, анализ и документирование всех доступных данных о произошедшем инциденте.[1] Основная цель здесь — не только фиксация ущерба или потенциального ущерба от атаки, но и извлечение уроков, которые помогут предотвратить подобные инциденты в будущем.

Как только атака идентифицирована, специалисты по кибербезопасности приступают к детальному анализу методов и инструментов, использованных злоумышленниками. Это включает в себя изучение векторов атаки, таких как способы доставки фишинговых сообщений, использование вредоносных ссылок или вложений, а также методы маскировки и обхода защитных механизмов. Анализируя эти данные, команда безопасности может выявить уязвимые места в текущей системе защиты и разработать рекомендации по их устранению.

После сбора и анализа информации следует этап отчетности. Составление подробных отчетов о фишинговых атаках и их последствиях позволяет руководству организации и специалистам по безопасности оценить масштаб проблемы и эффективность внедренных мер безопасности. Отчеты могут включать в себя описание использованных атакующими методик, идентифицированные уязвимости, оценку ущерба, а также предложения по улучшению системы кибербезопасности.

Важным аспектом анализа и отчетности является обмен информацией не только внутри организации, но и с внешними структурами, такими как правоохранительные органы, другие компании и специализированные сообщества по кибербезопасности. Это позволяет расширить базу данных о фишинговых атаках, способствовать кооперации в борьбе с киберпреступностью и повысить общий уровень защищенности в цифровом пространстве.

Таким образом, анализ и отчетность не только фиксируют опыт борьбы с фишингом, но и способствуют накоплению знаний, которые могут быть использованы для предотвращения будущих атак, повышения устойчивости инфраструктуры и формирования культуры кибербезопасности среди пользователей и сотрудников

Фишинг остается одной из наиболее распространенных и эффективных форм кибератак, наносящих значительный ущерб как отдельным лицам, так и организациям. Распознавание признаков фишинга, применение мер предосторожности и постоянное обучение являются ключевыми элементами защиты от этих угроз. В то время как технологии безопасности продолжают развиваться, осознанное отношение к кибербезопасности и проактивные действия пользователей играют решающую роль в обеспечении безопасности в цифровом мире.

Список литературы

1. Гельфанд А. М. и др. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе //Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2018. – №. 8. – С. 91-97.
2. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO //Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.
3. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения–Информационные технологии и телекоммуникации, 2021 //Т. – 2021. – Т. 9. –С. 1-2
4. Катасонов А. И., Штеренберг С. И., Цветков А. Ю. Оценка стойкости механизма, реализующего... Мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства gnu linux //Вестник Санкт-Петербургского

государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 2. – С. 50-56.

5. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411

References

1. Gelfand A.M. et al. Development of a model for the distribution of self-modifying code in a protected information system //Modern science: actual problems of theory and practice. Series: Natural and Technical Sciences. – 2018. – No. 8. – pp. 91-97.
2. Krasov A.V. et al. Packet switching methods in CISCO networks //Materials of the All-Russian scientific and practical conference "National Security of Russia: current aspects of the "GNII" National Development". July 2018. – 2018. – pp. 31-35.
3. Shterenberg S. I., Moskalchuk A. I., Krasov A.V. Development of security scenarios for creating vulnerable virtual machines and studying penetration testing methods–Information technologies and Telecommunications, 2021 //Vol. – 2021. – vol. 9. –pp. 1-2
4. Katasonov A. I., Shterenberg S. I., Tsvetkov A. Yu. Assessment of the stability of the mechanism implementing... The mandatory essential role model of access rights differentiation in gnu linux operating systems //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – No. 2. – pp. 50-56.
5. Budarny G. S. et al. Types of security breaches and typical attacks on the operating system //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 406-411.