St. Cyril and St. Methodius University of Veliko Tarnovo
Faculty of Economics

ФИШИНГОВЫЕ АТАКИ В ИНТЕРНЕТ-БАНКИНГЕ

PHISHING ATTACKS IN ONLINE BANKING

Венелина Цаневска
Venelina Tsanevska

Великотърновски университет „Св. св. Кирил и Методий“
St. Cyril and St. Methodius University of Veliko Tarnovo

Abstract: Phishing is a cybercrime in which the attacker (hacker) imitates a real person or an institution, most often through e-mail or other means of communication. In this type of cyberattack, the attacker sends malicious links or attachments through phishing e-mails, which can perform various functions and lead to various consequences, including loss of personal funds and identity theft. In this context, the banking sector, which is continuously more sophisticated and digitized, is becoming increasingly vulnerable to such attacks. Phishing attack detection, prevention and protection are issues that are increasingly on the agenda. The current publication addresses these questions. The first part of the publication clarifies the nature of phishing attacks and the technologies used to breach bank security. Some of the more important possible attacks are discussed - “Man-in-the Middle Attack”, “Deceptive Phishing Attack”, “Malware-based Phishing”, “DNS-Based Phishing”. The second part of the article focuses on possible solutions against phishing attacks. Recommendations for improving banks’ protection mechanisms are outlined.

Keywords: phishing, phishing attacks, online banking, technology, banking security
JEL: G21

ВСТУПЛЕНИЕ

Сегодня использование Интернета облегчает повседневную жизнь людей. Некоторые сайты в Интернете устаревают и умирают из-за невозможности обновления своих функциий и, следовательно, их полезности для пользователей, но на других разработчики постоянно адаптируют функции, добавляя ценность и удовлетворяя все больше потребностей пользователей (Kostadinova, & Kolev, 2020, p. 461). В последние годы, с развитием цифровых технологий и распространением социальных сетей, общение между людьми стало проще, но это привело к большей опасности непреднамеренного сбора и использования обмениваемой информации.

Банковское дело – один из секторов экономики, который добился больших успехов в этом отношении и который неимоверно развился. Появление интернет-банкинга и его постепенное совершенствование позволило банкам предложить своим клиентам удобное и гибкое банковское обслуживание в режиме реального времени из любой точки мира.

Интернет-банкинг хороший инструмент как для банков, так и для их клиентов. Для клиентов удобно иметь доступ к различным банковским продуктам и услугам без необходимости физического посещения филиала банка, а в то же время кредитные организации снижают часть своих операционных расходов.

С помощью интернет-банкинга банки предоставляют своим клиентам ряд удобных возможностей, но это влечет за собой потенциальные проблемы с безопасностью. В постепенно оцифровывающейся жизни компьютерные хакеры совершенствуют свои способы атаки и разрабатывают различные методы финансовых злоупотреблений. Предложение услуг онлайн-банкинга увеличи-

вается, но в то же время увеличивается и количество хакерских атак через банковские системы. Одной из таких атак, которую можно определить как наиболее распространенную, является так называемый «фишинг». Обнаружение фишинговых атак с высокой точностью является одним из важнейших исследовательских вопросов в области кибербезопасности.

1. Фишинговые атаки и технологии в интернет-банкинге

Оцифровка – это инструмент, обеспечивающий доступ к информацию в глобальной сети и тем самым приводящий к созданию и применению новых форм и стандартов защиты авторских прав и интеллектуальной собственности (Mancheva, 2021, p.3). Это среднесрочный и долгосрочный процесс, при котором видимые результаты приходят после многих лет напряженной работы (Byanov, & Byqnova, 2022, p. 371). Развитие банковского сектора в направлении цифровизации и ежедневное использование электронной почты (e-mail) для служебного общения в последние годы является предпосылкой ряда злоупотреблений в онлайн-пространстве. Именно с этим связана одна относительно новая концепция – социальная инженерия. Социальная инженерия – это широкий термин, используемый для описания ряда методов, используемых для обмана людей, чтобы они предоставили мошенникам (хакерам) в онлайн-среде информацию, которой они требуют.

Одной из самых распространенных угроз, с которыми сталкиваются люди, является фишинг с помощью социальной инженерии. Фишинг начался в начале 1990-х как способ хакеров получить учетные записи в американской интернет-службе и медиа-компании (America Online, AOL). Термин фишинг впервые был использован в 1996 году. В настоящее время слово “фишинг” широко используется с тысячами упоминаний в научной литературе, медиапространстве и коммерческих банках. “Фишинг” *(“phishing”)* происходит от английского слова *„fishing“* (ловить рыбу), т.е. это вариант слова “рыбалка”. Идея состоит в том, что пользователь “клюнет” на приманку (имейл или сайт обмена мгновенными сообщениями, который перенаправит пользователя на вредоносные фишинговые веб-сайты). Таким образом, фишинг определяется как конкретный метод, осуществляемый в основном по электронной почте и предназначенный для кражи конфиденциальной информации о данных пользователя, в том числе учетные данные и номера банковских карт.

В последние годы наблюдается тенденция к увеличению количества вредоносных программ, при этом фокус ставится на уязвимые места в системах онлайн-банкинга. Некоторые авторы отмечают, что фишинг – это искусство обмана и что современные более изощренные фишинговые атаки призваны казаться более законными, чем когда-либо в их истории (Vega, Shevchyk, & Cheng, 2022). Это приводит к необходимости надежных моделей безопасности в банках. Именно из-за этого необходимо выявить существующие методы атаки. Кроме того, следует учитывать, что ответственность за поддержание безопасности всегда переносится на самое слабое звено в цепи безопасности, под которым в большинстве случаев понимается конечный пользователь.

Фишинговые атаки постепенно стали одними из самых распространенных финансовых преступлений.

В научной литературе представлен ряд исследований, посвященных тестированию различных сценариев фишинговых атак. Например, в своей работе Sahoo (Sahoo, 2021, p.3) представил результаты исследования с постановкой целевой фишинговой атаки. Атаковали 120 сотрудников по электронной почте, в которой им сообщали, что их электронные банковские счета подвержены высокому риску атаки, и предлагали немедленно войти в свою учетную запись по прикрепленной фальшивой ссылке, чтобы проверить свой баланс. Сотрудники, которых успешно обманули, составляют 44% выборки. Еще интереснее тот факт, что 8 из сотрудников (или 7% выборки) работают информационно-техническими аудиторами и сотрудниками информационно-технического отдела (ИТО). Эксперимент показывает, что фишинг крайне опасен для всего общества, так как жертвами стали почти половина ответивших сотрудников, в том числе и более узкие специалисты из сферы информационных технологий.

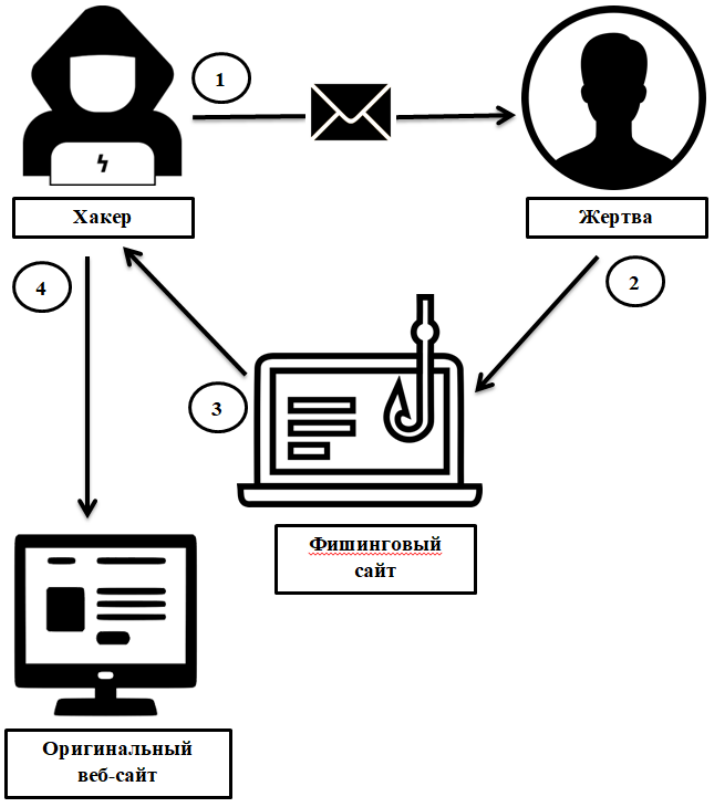
Чтобы предложить модели и решения безопасности, необходимо сначала правильно понять и классифицировать существующие методы атаки и уязвимости, на которых они основаны. В настоящее время существуют различные передовые технологии для взлома безопасности банковских систем.

Один из них это ***„Man-in-the Middle Attack“***. По сути, хакеры стоят между банком и его клиентами, в то время как последние используют свои банковские счета в Интернете. В этой атаке злоумышленник тайно передает и, возможно, изменяет переписку между двумя сторонами, которые считают, что общаются друг с другом напрямую (Mallik, Ahsan, Shahadat, & Tsou, 2019, p.77). В этом случае ни банк, ни его пользователи не догадываются о том, что транзакции связаны с фишинговыми атаками, до тех пор, пока деньги не исчезнут со счета клиента без его разрешения. Хакеры, воспользуются с одной стороны возможностями онлайн-сервисов, а с другой – неосведомленностью пользователей о фишинговых атаках.

Другой известный метод фишинга известен как ***„Deceptive Phishing Attack“*** (Prakasam, & Chithralekha, 2022, p. 453–454), при котором действия направлены на получение доступа к банковским счетам клиентов. Наиболее часто используемый метод заключается в отправке поддельных уведомлений по электронной почте клиентам банка, при этом хакер притворяется, что представляет банк, или придумывает фиктивные сценарии, чтобы убедить клиента посетить указанный веб-сайт. Соответственно, в письме указывается поддельная ссылка (веб-адрес) на вредоносный сайт, а чаще всего в адресе страницы буквы заменяются цифрами или наоборот (например, буква “о” заменяется нулем). Иногда есть дополнительные тексты, направленные на звонок, что внушает дополнительное ощущение срочности. Цель состоит в том, чтобы получатель щелкнул на указанную веб-ссылку. В этом случае клиент банка перенаправляется на мошеннический веб-сайт, который сильно модифицирован, но выглядит как официальный сайт банка. Поскольку это не оставляет сомнений, на следующем шаге пользователь может ввести свое имя пользователя и пароль. В этот момент злоумышленник уже получает доступ к конфиденциальной информации пользователя и может совершить ряд незаконных действий в личных целях.

Поэтому классическую схему фишинга можно свести к следующим шагам (рис. 1):

1. Атакующий хакер отправляет электронное письмо целевой жертве.
2. Жертва нажимает на письмо и переходит на фишинговый сайт.
3. Хакер собирает учетные данные жертвы.
4. Хакер использует учетные данные жертвы для доступа к исходному веб-сайту.



Рус. 1. Классическая схема фишинга

Суть в том, что конечные клиенты рискуют понести финансовые потери, если поспешно отреагируют на такое письмо.

Другой известеный метод фишинга основан на вредоносном программном обеспечении – ***"Malware-based Phishing".*** Это делается с помощью программ, которые устанавливаются на компьютер клиента. Взломанная технология может установится когда клиенты или сотрудники банков посещают неавторизованные веб-сайты или устанавливают зараженные программные обеспечения на своих персональных компьютерах. Фишинговые атаки могут быть использованы с помощью различных методов, чтобы получить достоверную информацию о банковских операциях пользователя (таким методом может быть так называемый кейлоггер). Это программы, которые устанавливаются на компьютеры пользователей банка без их знания и разрешения. С этой точки зрение, этот вид вредоносных программ легко использовать, так как жертвы часто не знают, что такое программное обеспечение существует на их компьютерах. Кейлоггер отслеживает и записывает нажатия клавиш. Таким образом, программное обеспечение получает информацию и отправляет ее хакеру, который анализирует нажатия клавиш, чтобы найти имена пользователей и пароли.

Еще одна известная афера – это так называемая "pharming", при котором осуществляется контроль над данными пользователей банка. Это фишинг на основе DNS ***(„DNS-Based Phishing)***. При этой атаке настройки DNS изменяются неуполномоченным образом, таким образом перенаправляя клиентов банка на мошеннические и/или зараженные сайты (Tsanevska, 2019, p. 175), которые выглядят законными. То есть эта форма атаки перенаправляет пользователей на поддельный веб-сайт, когда они пытаются ввести доменное имя веб-адреса своего банка. Атака может осуществляться двумя способами – злоумышленники могут установить вирус на компьютер пользователя или подделать веб-домен банка.

2. Возможные решения против фишинговых атак

Существует ряд методов, которые любой банк может использовать для борьбы с фишинговыми атаками, некоторые из которых описаны в следующем разделе.

Персонализация электронной почты

Самый простой способ для банков бороться с мошенническими фишинговыми сообщениями – персонализировать их для конкретных клиентов банка. Кроме имени клиента информация может также включать уникальную информацию, известную только банку и клиенту. Возможное решение – начинать каждое электронное письмо от банка с имени клиента. Это учит клиента быть осторожным и знать, что электронное письмо, в котором не указано его имя, скорее всего, является мошенничеством. Фишинговые атаки не связаны с личной информацией пользователей, и это способ уменьшить количество попыток мошенничества.

Настройка веб-страницы

Другой способ – персонализация веб-страницы банка таким образом, чтобы клиенты использовали личную распознаваемую информация – текст или изображение рядом со своими паролями и именами пользователей. Кроме того, пользователям может быть предоставлена возможность ввести свое имя пользователя и пароль на двух отдельных страницах. Это разделение на два этапа может затруднить выполнение атак. Таким образом, вторая страница открывается только тогда, когда введенное имя пользователя действительно. Вторая страница является личной и поддерживается определенными словами или изображениями, которые пользователь выбрал при создании своей учетной записи.

Программное обеспечение безопасности

Пользователи будут защищены, если они используют разные программные продукты. Возможный вариант – в состав программного обеспечения входят различные компьютерные программы, которые защищают пользователей от вирусов и шпионских программ, сканируя целые файлы. Хорошим решением является использование программного обеспечения для защиты от логирования (anti-logger software), которое должно быть установлено с обеих сторон – клиентом и банком. Его цель – помочь обнаружить скрытые программы-кейлоггеры.

Осведомленность клиентов

Осведомленность клиентов также очень полезна в процессе предотвращения хакерских атак. В связи с этим банкам рекомендуется регулярно информировать своих клиентов об опасности фишинговых атак и эффективных мерах противодействия. Для кредитных организаций целесообразно информировать своих клиентов о способах, которыми они будут с ними общаться, еще при первой встрече с ними, а кроме того, визуализировать инструкции на официальном сайте банка до того, как клиент войдет в свой банковский профиль. Кроме того, учреждения могут также предлагать обучение своим клиентам. Таким образом, все программные подходы к ограничению фишинговых атак будут сопровождаться обучением пользователей, чтобы помочь людям лучше распознавать поддельные электронные письма и веб-сайты (Mustafa, Mustafa, & Hamdani, 2021, p. 31).

Многофакторная аутентификация

Многофакторная аутентификация – важный инструмент для обеспечения кибербезопасности в Интернете. Кредитные учреждения должны использовать эффективные методы для аутентификации личности клиента. С развитием электронного банкинга произошел постепенный переход от однофакторной аутентификации к двухфакторной аутентификации. По своей сути двухфакторная аутентификация требует, чтобы пользователи подтверждали свою личность несколькими независимыми методами. Дополнительные учетные данные проверки связаны с:

- то, что знает пользователь;
- то, что есть у пользователя;

Первый фактор – это “то, что знает пользователь”. Факторы этого типа являются наиболее распространенными и наиболее уязвимыми для атаки. Они менее безопасны, потому что информацию легче передать или украсть. Примеры аутентификации того, что известно пользователю, включают:

• пароли
• ПИН-коды
• ответы на секретные вопросы (например, “Где ты родился?”, “Как зовут твоего первого учителя?”, “Как зовут твоего питомца?” и т. д.).

Второй фактор – это “то, что есть у пользователя”, и этот тип факторов также называют факторами владения, т.е. они относятся к информации, которую вы можете физически носить с собой. Обычно это аппаратное или программное обеспечение, с помощью которого пользователь банка получает электронный уникальный код или пароль.

Цель двухфакторной аутентификации – гарантировать, что пользователи, осуществляющие доступ к банковской системе, являются реальными пользователями. Таким образом, чтобы войти в безопасную программу, пользователю должен ввести пароль (то, что знает пользователь) и ввести уникальный аппаратный код (то, что есть у пользователя). Фишинговые атаки могут легко перехватить пароль пользователя, поэтому двухфакторная аутентификация эффективна для их предотвращения. Только правильный пароль в сочетании с правильным номером из правильного аппаратного тега предоставит пользователю доступ.

С улучшением электронного банкинга все чаще говорят о третьем факторе, а именно: “то, чем является пользователь”. Это связано с биометрической верификацией, посредством которой человека идентифицируют по его уникальным биологическим признакам. Биометрические данные используются для предоставления уникальной идентичности различным лицам (Eneji, Ekwegh, Basil, & Gospel, 2019, p. 9551). Примеры биометрической верификации включают:

• отпечаток пальца
• ладонь
• голос и лицо
• сканирование сетчатки и радужной оболочки
• подпись
• ДНК

Учитывая возрастающий характер фишинговых атак, вполне вероятно, что коммерческие банки постепенно начнут задумываться о дальнейшем увеличении количества элементов проверки. Например, в будущем может быть добавлен четвертый фактор, не столь известный, как вышеупомянутый, а именно “там, где вы находитесь”, т.е. этот фактор связан с местонахождением конечного пользователя. Самый известный метод определения местоположения пользователя – через его IP-адрес. Если при настройке своего банковского счета он укажет, что живет в Болгарии, и кто-то попытается взломать его из Англии, то он будет уведомлен об этой злонамеренной попытке.

Все чаще говорят о другом, пятом факторе – “то, что делаеште”. Это тип аутентификации, который подтверждает личность путем наблюдения за действиями. Эти действия могут быть жестами или прикосновениями. Например, у пользователей Windows 8/10 есть такая опция, и она известна под названием “picture password”. Это позволяет пользователю устанавливать жесты/прикосновение к изображению в качестве способа аутентификации, а затем использовать эти жесты в качестве пароля. В самом общем случае это происходит путем первоначальноto выбора картинки, а затем пометки ее действиями (рисованием круга или линии, или просто нажатием на определенное место).

ЗАКЛЮЧЕНИЕ

Использование интернет-банкинга связано с различного рода рисками, и особое внимание следует уделять фишинговым атакам, которые могут нанести особый вред как банкам, так и потребителям, которые не принимают меры предосторожности против попыток такого рода мошенничества. В заключение следует отметить, что фишеры становятся все умнее, а процедуры и приемы, используемые при фишинге, постоянно развиваются. Ожидается, что будущие поколения атак станут более масштабными и изощренными. Злоумышленники разрабатывают новые методы обхода протоколов безопасности, чтобы повысить шансы на успешную атаку. В дополне-

ние к неспособности пользователя обнаруживать фишинговые атаки, частота атак и разнообразие методов помогают повысить шансы на успешные атаки. Технологические достижения и недавно обнаруженные уязвимости также играют важную роль в успехе фишинговых атак.

Фишинг не может быть преодолен с помощью только одного решения. В ответ банки должны регулярно обновлять свои меры безопасности и обеспечивать безопасность транзакций между собой и своими клиентами. Финансовые учреждения должны уделять особое внимание защите информации собственной организации, пользователей и их личных финансов, которыми могут воспользоваться хакеры. Финансовые учреждения должны использовать обновленные меры противодействия, такие как двухфакторная (или более высокая) аутентификация, наряду с другими программами защиты клиентов.

В значительной степени фишинговые атаки не могут быть остановлены только с помощью технологий, поэтому клиенты банка тоже должны быть подозрительными и осторожными при работе с личными средствами в онлайн-среде. В связи с этим рекомендуется периодически информировать пользователей о рисках фишинговых атак и о способаь, при помощи которых может произойти неуполномоченный доступ к их финансовой информации.

REFERENCES

1. Byanov, I. & Byanova, N. 2022. Digitization of the Bulgarian economy in the European Union. *In: Proceedings of jubilee scientific conference on the occasion of 85 years of "General Economic Theory" Department: Economics and economic theory: issues and interactions*, Varna: Science and Economics, p. 371

2. Eneji, S. & Ekwegh, E. & Basil, O. & Gospel, A. 2019. Enhanced Platform for the Application of Biometric Security in Electronic Banking: Case Study of Nigeria. *Asian Journal of Science and Technology,* Vol. 10, Issue, 03, p. 9551

3. Kostadinova, N. & Kolev, D. 2020. Digital communication toolset for organized event markets in hospitality business, *Collection of papers from jubilee scientific conference "Tourism and connectivity"*, Varna: Science and Economics, DOI: https://doi.org/10.36997/TC2020.461, p. 461

4. Mallik, A. & Ahsan, A. & Shahadat, M. & Tsou, J. 2019. Man-in-the-middle-attack: Understanding in simple words. *International Journal of Data and Network Science,* 3(2), p. 77

5. Mancheva-Ali, O. 2021. The role of digitization in tourism. In: *Strategiczne perspektuvy rozwów pośćięciego biznesu*, p. 38

6. Mustafa, M. & Mustafa, E. & Hamdani, K. 2021. Effectiveness of Online Anti-Phishing Delivery methods in raising Awareness among Internet Users. *Master`s thesis*, p. 31

7. Prakasam, Ch. & Chithralekha, T. 2022. A literature review on classification of phishing attacks, *International Journal of Advanced Technology and Engineering Exploration*, 9(89):446-476, p. 453-454

8. Sahoo, P. 2021. An Emerging Solution for Detection of Phishing Attacks. In: *Cybersecurity Threats with New Perspectives*, p. 3

9. Tsanevska, V. 2019. E-banking as an important function in today's world. In: *Collection of studies Economic Horizons '21 - financial and accounting perspectives, volume I*, Veliko Tarnovo: Publishing house "St. Cyril and St. Methodius University of Veliko Tarnovo", p. 175

10. Vega. J. & Shevchyk, D. & Cheng, Y. 2022. A Literature Survey of Phishing and Its Countermeasures. In: *Conference: Second Annual Computer Science Conference for CSU Undergraduates*

https://dojowithrenan.medium.com/the-5-factors-of-authentication-bcb79d354c13, viewed 5 March 2024

За контакти:
Венелина Цаневска, главен асистент, доктор
Служебен адрес: В. Търново, ул. „Арх. Георги Козарев" 1, корпус 4
ВТУ „Св. св. Кирил и Методий", Стопански факултет
Катедра „Финанси и счетоводство"
Ел. поща: v.tsanevska@ts.uni-vt.bg