SATBAYEV UNIVERSITY

Computing & Engineering

Volume 2 (2024), Issue 1, 14-18

https://doi.org/10.51301/ce.2024.i1.03

Social networks as an attack vector for targeted attacks

A. Yerkebay*, Kh. Yubuzova, Zh. Seitkaliyeva

Satbayev University, Almaty, Kazakhstan

**Corresponding author: abylay.erkebay@stud.satbayev.university*

Abstract. This research paper thoroughly examines the issue of phishing on social media platforms and the various vulnerabilities inherent in these systems. Phishing is a widely used social engineering technique employed by attackers to deceive users into revealing sensitive information, such as login credentials or financial data. The work provides a detailed analysis of the different types of phishing attacks, including traditional email phishing, spear phishing, whaling, and the more targeted approach of social media phishing. Particular attention is given to the mechanisms of phishing within social networks, such as advanced social engineering tactics, the dissemination of fraudulent links, deceptive messages, and the practice of account cloning. Additionally, the study delves into the critical vulnerabilities of social media platforms, including insufficient account security measures, the proliferation of fake profiles, the general lack of user awareness, and underlying technical vulnerabilities within the platforms themselves. Lastly, the paper suggests comprehensive methods to protect against phishing, including improving user education and awareness, adopting two-factor authentication, regularly updating passwords, reporting suspicious activities, and implementing stronger technical safeguards. The study underscores the importance of collaborative efforts between users and social network providers to effectively combat phishing and promote greater internet security.

Keywords: *phishing, social networks, fraud.*

1. Introduction

Phishing on social media is one of the most common, pervasive, and serious threats that affect both individual users and organizations alike [1]. Social networks such as Facebook, Instagram, Twitter, and LinkedIn, while serving as valuable platforms for communication, information sharing, and fostering interaction, also create an environment ripe for exploitation by cybercriminals. These platforms have grown to become an integral part of daily life, connecting millions of users worldwide, but this widespread usage has also increased their attractiveness as targets for phishing attacks and other malicious activities [2]. In this research paper, we will take an in-depth look at the sophisticated phishing mechanisms that are commonly employed on social media platforms, exploring how attackers manipulate trust and exploit the inherent social nature of these networks to deceive users into revealing sensitive information, such as passwords, personal data, or financial details. We will examine a variety of tactics, including the use of fraudulent links, fake profiles, direct messages, and posts designed to lure victims into phishing traps. Additionally, this paper will analyze the underlying vulnerabilities that make social media platforms particularly susceptible to such attacks. These include factors such as insufficient account security measures, weak user authentication protocols, and the overall lack of awareness among users regarding potential phishing threats [3]. Furthermore, the inherent openness and interconnectedness of social networks make it easier for attackers to impersonate legitimate users or organizations, adding another layer of complexity to the threat landscape. This study aims to provide insights into why phishing on social media remains a persistent problem and will suggest potential countermeasures to mitigate the risks.

2. Materials and methods

2.1 Tools Used

In conducting the research for this article, we employed a variety of specialized tools that are essential for cybersecurity investigations. The primary tool utilized was Kali Linux [4], a widely recognized Linux distribution specifically designed for advanced security tasks. Its robust environment allowed me to simulate various attack vectors and assess vulnerabilities in different systems.

Additionally, we utilized the Metasploit Framework [5], a powerful platform for developing, testing, and executing exploit code against remote target machines. Metasploit provides a comprehensive suite of tools that facilitate the identification of security weaknesses, enabling researchers to understand how vulnerabilities can be exploited in real-world scenarios.

Furthermore, we employed Maltego [6], a tool known for its capabilities in data mining and link analysis. Maltego allowed me to visualize relationships between different entities, such as individuals, organizations, and their online presence. This capability was instrumental in mapping out the threat landscape and identifying potential attack vectors, thereby enriching the analysis presented in this article.

By integrating these powerful tools into my research methodology, we were able to gather comprehensive data, conduct in-depth analyses, and draw more informed conclusions regarding the security challenges addressed in this study.

2.2 Research Objectives

The purpose of this paper is to comprehensively analyze social media phishing and related vulnerabilities and to develop recommendations to protect users and improve security on these platforms. To achieve this goal, the following tasks are considered:

1. Definition and Classification of Phishing: To study the different types of phishing, with a special focus on the methods used in social media.
2. Analysis of Phishing Mechanisms: To identify the main techniques and methods that attackers use to carry out phishing attacks on social media.
3. Identification of Social Media Vulnerabilities: To identify and describe the main vulnerabilities that make social media attractive for phishing attacks.
4. Development of Defense Recommendations: To propose effective measures and strategies to protect users and social media platforms from phishing.
5. Raising Awareness: To emphasize the importance of educating and raising user awareness of the risks and methods of protection against phishing.

The research aims to provide a deeper understanding of the threats associated with social media phishing and to help develop more effective security measures to protect users in the digital space.

3. Results and discussion

3.1 Vulnerability in vk.com

There exists a critical vulnerability within the popular social network VKontakte [7], a Russian social media platform founded in 2006 by Pavel Durov. This vulnerability allows all sent documents (files) to be accessed in an unprotected manner, rendering them open and available to unauthorized users. Consequently, this issue poses a significant privacy risk, as any files shared between users—irrespective of their sensitivity or intended audience—can be easily viewed or downloaded by individuals without proper authorization. This lack of security not only compromises personal information but also undermines user trust in the platform (Figures 1-2).

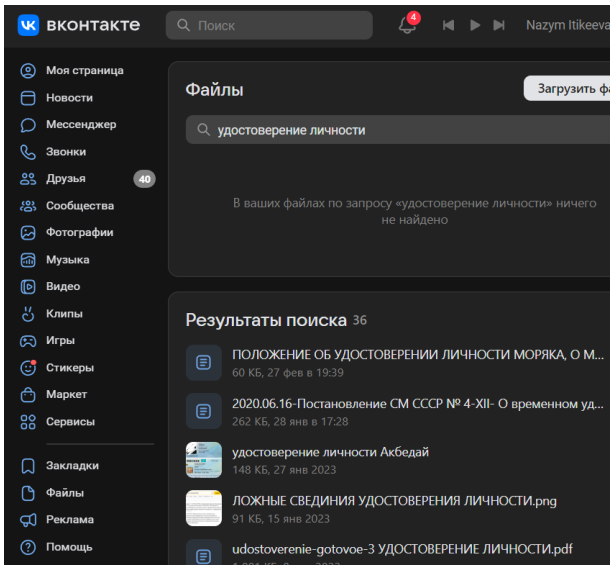

Figure 1. Searching files by keywords

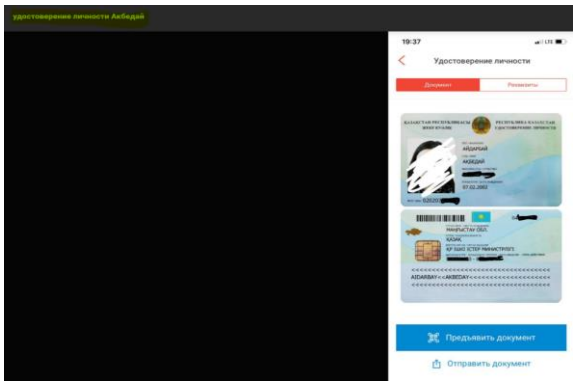

Figure 2. Identity card in open form

3.2 Targeted phishing

If an attacker has found personal data on the Internet, they can use stolen passport data to gain access to bank accounts, credit cards, or other personal accounts. To protect against such attacks, it is important to monitor the security of personal data on the Internet, use strong passwords, two-factor authentication, be attentive to suspicious requests, and, most importantly, do not share personal data on social networks [8]. In practice, we can also encounter targeted phishing (Figures 3-4). Targeted phishing attacks are designed to use personal information to make the targeted victim click on a link. They also sometimes use urgency or the risk of monetary value to lure their victims.

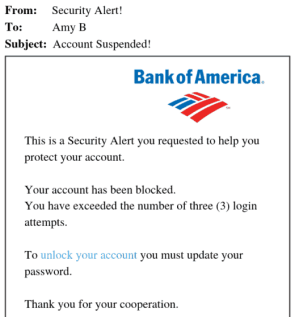

Figure 3. Targeted attack

For example, an email from Bank of America shows that someone has tried to access Amy's account and that the bank has blocked it. For Amy to solve the problem, all she has to do is click on a link to reset her password. The attackers hope that Amy will panic about her money, click on the link, and then give them her login information.

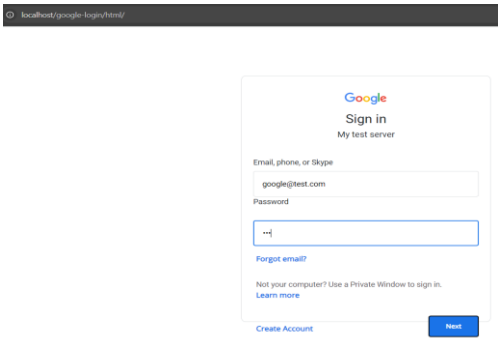

Figure 4. Phishing site for data theft

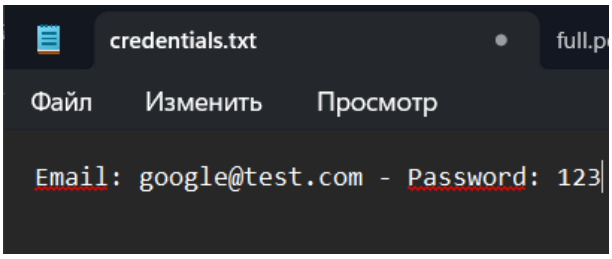

Figure 5. Stolen credentials

3.3 Links for collecting information and downloading the malware

Such web servers can be configured on third-party servers and subsequently sent to target users via email. It is essential to exercise caution when receiving emails that claim to offer giveaways, prizes, or similar incentives, as these may be phishing attempts. In the example provided below (Figure 6), a closer examination reveals a suspicious link embedded within the message. The URL in question is not affiliated with the official Halyk organization, which indicates the likelihood of fraudulent intent. Careful analysis of such links is crucial to avoid falling victim to phishing schemes.

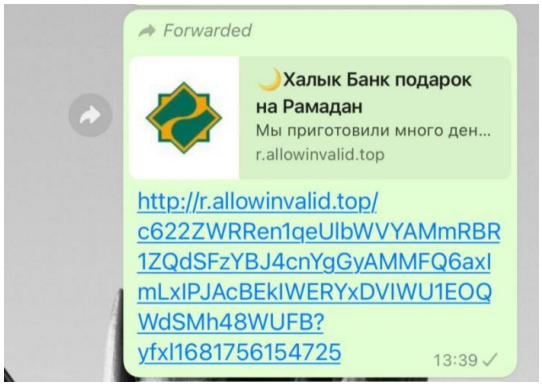

Figure 6. Malicious mailing on the WhatsApp messenger

The mailing contains an embedded link, which, when clicked, takes the potential victim to a website where they are required to answer questions and take part in a draw. To receive a cash prize, potential targets need to send a message with a link to their friends and family.

Metadata is information about data, which can include details such as the time and place of file creation, authorship, file versions and changes, technical parameters, etc. If an attacker gains access to metadata, they can do the following:

1. Personal identification: Metadata can contain information about the author of the file (for example, the username of the computer or device), which helps the hacker identify the owner of the file.

2. Location tracking: Metadata for photos and videos can contain GPS coordinates, which allows the hacker to find out the target's location and travel routes.

3. Targeted attacks: Knowing details about the victim's activities and contacts, a hacker can carry out more accurate and effective phishing or social engineering attacks.

4. Espionage and information gathering: Metadata can be used to gather information about the projects and documents the person is working on, which is useful for industrial espionage or preparing attacks on the targeted organization.

5. Remote access and vulnerability exploitation: Metadata can contain information about software and operating system versions, allowing a hacker to search for and exploit known vulnerabilities.

According to the comprehensive Kaspersky Internet Security for Android 2021-2023 report [9], a total of 341,954 attempts to click on phishing links from various messaging platforms were successfully blocked. The data shows that WhatsApp users were responsible for the vast majority of these attempts, with 90.00% of the blocked links originating from this platform. Telegram ranks second with 5.04%, followed closely by Viber users, who accounted for 4.94% of the blocked phishing links. These findings highlight the significant risks associated with phishing attacks across widely used messenger applications, emphasizing the importance of heightened security awareness among users.

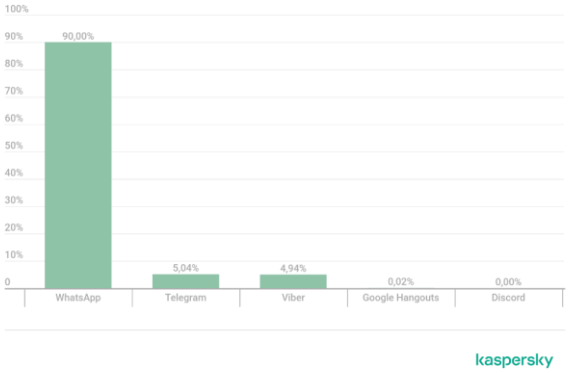

Figure 7. Phishing in messengers

3.4 Social Media Phishing Protection Recommendations

1. User Education and Awareness: Training and education on recognizing phishing attacks should be provided and precautions taken, such as verifying the authenticity of links and messages [10].

2. Using Two-Factor Authentication: Two-factor authentication makes it much more difficult for attackers to gain access to user accounts.

3. Regularly Updating Passwords: Users should change their passwords regularly and use unique passwords for different accounts.

4. Reporting Suspicious Activity: Social networks should provide users with convenient mechanisms to report suspicious activity and fake profiles.

5. Technical Measures: Social networks should constantly update their security infrastructure, patch vulnerabilities, and implement modern protection methods, such as content filtering and activity monitoring.

4. Conclusions

Phishing remains one of the most used techniques by fraudsters to illegally obtain sensitive personal information from users. This information may include phone numbers, age, names, as well as critical financial data such as payment card details (16-digit card number, expiration date, and 3-digit CVV code). In addition, attackers often target logins and passwords from banking mobile applications and personal accounts on various platforms. Given the increasing

sophistication of phishing attacks, it is essential for users to stay vigilant and take necessary precautions.

To reduce the risk of falling victim to phishing, I recommend thoroughly educating individuals on the different types of phishing attacks and regularly updating their knowledge of evolving threats. Awareness of how phishing works can help in recognizing suspicious messages, emails, or links that may seem legitimate at first glance. It is equally important to be cautious when sharing personal data on the internet, particularly on social media or in public forums, as these platforms are often targeted by cybercriminals. By staying informed and cautious, users can significantly reduce the likelihood of their personal information being compromised by phishing scams.

Acknowledgements

Author would like to express my sincere gratitude to my academic supervisor, Yubuzova Khalicha Ibragimovna for their invaluable guidance and support throughout the research process.

References

[1] Grigoriev, I.V. (2019). Information Security: Textbook. *St. Petersburg: Piter*
[2] Vershinin, S.V. (2020). Cybercrime and Information Security. *Moscow: Academy*
[3] Kaspersky Lab. (2019). Phishing: How to Protect Yourself. *Retrieved from:* www.kaspersky.ru
[4] Beekman, G. (2019). Kali Linux Revealed: Mastering the Penetration Testing Distribution. *Nobel Press*
[5] Gallagher, D.K. (2020). Metasploit: The Penetration Tester's Guide. *San Francisco*
[6] Goudar, S. (2020). Maltego: A Complete Guide.
[7] VKontakte. Official website: www.vk.com
[8] Symantec Corporation. (2002). Internet Security Threat Report. *Retrieved from*: https://docs.broadcom.com/doc/istr-03-jan-en
[9] Anti-Phishing Working Group (APWG). (2023). Phishing Activity Trends Report. *Retrieved from*: https://apwg.org/trendsreports/
[10] Facebook Security. Protecting People from Phishing.facebook.com

Мақсатты шабуылдар үшін әлеуметтік желілердегі шабуыл векторы

А. Еркебай*, Х. Юбузова, Ж. Сейітқалиева
Satbayev University, Алматы, Қазақстан
**Корреспонденция үшін автор: abylay.erkebay@stud.satbayev.university*

Аңдатпа. Бұл ғылыми мақала әлеуметтік желілердегі фишинг мәселесін және осы платформалардағы осалдықтарды жан-жақты талдайды. Фишинг – бұл шабуылдаушылар пайдаланушыларды алдап, құпия ақпаратты, мысалы, логин немесе қаржылық деректерді алуға бағытталған әлеуметтік инженерия әдісі. Зерттеуде фишинг шабуылдарының әртүрлі түрлері, соның ішінде дәстүрлі электрондық пошта арқылы фишинг, спар-фишинг, «ірі балық аулау» (whaling) және әлеуметтік желіде фишинг жасау талданады. Әлеуметтік желілердегі фишинг механизмдеріне ерекше назар аударылады, мысалы, жетілдірілген әлеуметтік инженерия әдістері, жалған сілтемелерді тарату, алдамшы хабарламалар және аккаунттарды көшіру тәжірибесі. Сонымен қатар, әлеуметтік желілердегі негізгі осалдықтар қарастырылады, соның ішінде аккаунттарды қорғаудың жеткіліксіздігі, жалған профильдердің көбеюі, пайдаланушылардың хабардарлығының төмендігі және платформалардың техникалық осалдықтары. Соңында фишингтен қорғанудың жан-жақты әдістері ұсынылады, соның ішінде пайдаланушылардың хабардарлығын арттыру, екі факторлы аутентификацияны қолдану, құпия сөздерді үнемі жаңартып отыру, күмәнді әрекеттерді хабарлау және күшейтілген техникалық қауіпсіздік шараларын енгізу. Зерттеу фишингпен тиімді күресу және интернет қауіпсіздігін қамтамасыз ету үшін пайдаланушылар мен әлеуметтік желі провайдерлерінің бірлескен күш-жігерінің маңыздылығын атап көрсетеді.

Негізгі сөздер: *фишинг, әлеуметтік желілер, алаяқтық.*

Социальные сети как вектор атаки для целевых атак

А. Еркебай*, Х. Юбузова, Ж. Сейітқалиева
Satbayev University, Алматы, Казахстан
**Автор для корреспонденции: abylay.erkebay@stud.satbayev.university*

Аннотация. В этой исследовательской работе подробно рассматривается проблема фишинга на платформах социальных сетей и различные уязвимости, присущие этим системам. Фишинг — это широко используемый метод социальной инженерии, используемый злоумышленниками для обмана пользователей с целью раскрытия конфиденциальной информации, такой как учетные данные для входа или финансовые данные. В работе представлен подробный анализ различных типов фишинговых атак, включая традиционный фишинг по электронной почте, целевой фишинг, уэйлинг и более целенаправленный подход фишинга в социальных сетях. Особое внимание уделяется механизмам

фишинга в социальных сетях, таким как продвинутые тактики социальной инженерии, распространение мошеннических ссылок, обманных сообщений и практика клонирования учетных записей. Кроме того, рассмотрены критические уязвимости платформ социальных сетей, включая недостаточные меры безопасности учетных записей, распространение поддельных профилей, общую неосведомленность пользователей и базовые технические уязвимости в самих платформах. Наконец, в статье предлагаются комплексные методы защиты от фишинга, включая повышение уровня образования и осведомленности пользователей, внедрение двухфакторной аутентификации, регулярное обновление паролей, сообщение о подозрительной деятельности и внедрение более жестких технических мер безопасности. В исследовании подчеркивается важность совместных усилий пользователей и поставщиков социальных сетей для эффективной борьбы с фишингом и повышения уровня безопасности в Интернете.

Ключевые слова: *фишинг, социальные сети, мошенничество*.

Received: 13 December 2023
Accepted: 16 March 2024
Available online: 31 March 2024