FarDU. Ilmiy xabarlar – Scientific journal of the Fergana State University

Volume 30 Issue 3, 2024-yil DOI: 10.56292/SJFSU/vol30_iss3/a130

UO‘K: 004.738.5

QOZOG‘ISTONDA KENG TARQALGAN FISHING HUJUMLARI VA FUQAROLARNI INTERNET FIRIBGARLARIDAN HIMOYA QILISH USULLARI

РАСПРОСТРАНЕННЫЕ ФИШИНГОВЫЕ АТАКИ В КАЗАХСТАНЕ И СПОСОБЫ ЗАЩИТЫ ГРАЖДАН ОТ ИНТЕРНЕТ-МОШЕННИКОВ

COMMON PHISHING ATTACKS IN KAZAKHSTAN AND WAYS TO PROTECT CITIZENS FROM INTERNET SCAMMERS

Raximov Quvvatali Ortikovich[1]
[1]Farg‘ona davlat universiteti, t.f.b.f.d., (PhD)

Mamatova Zilola Xabibulloxonovna[2]
[2]Farg‘ona davlat universiteti, p.f.b.f.d., (PhD)

Tazhikenova Nurzhanar Kabikenkizi[3]
[3]Evrosiyo milliy universiteti, Qozog‘iston, magistrant

Annotatsiya

Ushbu maqolada Qozog'istonda keng tarqalgan fishing hujumlari, ularni aniqlash va bartaraf etish usullari, foydalanuvchilarni xabardor etish va internet firibgarlariga qarshi samarali himoya choralarini ko‘rish usullari ko‘rib chiqilgan. Olib borilgan tadqiqotda mintaqada ko‘p uchraydigan eng mashhur fishing hujumlari tahlil etilgan. Qozog‘istonda uchraydigan o‘ziga xos tahdid va zaifliklarni aniqlash orqali internet foydalanuvchilarini onlayn muhitda duch keladigan xavf-xatarlar to‘liq yoritilgan. Maqolada fishing bilan bog'liq vaziyatni tahlil qilishdan tashqari, fuqarolarni bunday hujumlardan himoya qilish bo‘yicha profilaktika choralari ko‘rish usullari keltirilgan. Kiberxavfsizlik barqarorligini oshirish uchun individual va jamoaviy sa'y-harakatlarni amalga oshirish, mudofaa strategiyalari ishlab chiqish bo‘yicha tavsiyalar berilgan. Potentsial tahdidlarni aniqlash va ularni yumshatish uchun zarur bo‘lgan bilim va ko‘nikmalarni shakllantirish usullari ishlab chiqilgan. Ushbu maqolada keltirilgan xulosalar va tavsiyalar onlayn firibgarlar tomonidan qo‘llaniladigan doimiy o‘zgaruvchan taktikalarga qarshi o‘z himoyasini kuchaytirmoqchi bo‘lgan shaxslar va korxonalar uchun qimmatli manba bo‘lib xizmat qiladi.

Аннотация

В этой статье рассматриваются распространенные типы фишинговых атак на примере Казахстана, с целью повышения осведомленности и предложения эффективных мер защиты от интернет-мошенников. В исследовании анализируются наиболее популярные тактики фишинга, применяемые в регионе. Выявляя конкретные угрозы и уязвимости, уникальные для Казахстана, статья стремится дать читателям полное понимание рисков, с которыми они сталкиваются в онлайн-среде. Помимо анализа ситуации с фишингом, в статье рассматриваются превентивные меры по защите граждан от таких атак. Он дает практическое представление о стратегиях защиты, подчеркивая как индивидуальные, так и коллективные усилия по повышению устойчивости кибербезопасности. Статья призвана снабдить читателей знаниями, необходимыми для распознавания и смягчения потенциальных угроз. Выводы и рекомендации, представленные в статье, служат ценным ресурсом для частных лиц и предприятий, стремящихся укрепить свою защиту от постоянно меняющихся тактик, используемых интернет-мошенниками.

Abstract

This article examines common types of phishing attacks using Kazakhstan as an example, with the goal of raising awareness and suggesting effective protection measures against Internet scammers. The study analyzes the most popular phishing tactics used in the region. By identifying specific threats and vulnerabilities unique to Kazakhstan, the article strives to give readers a thorough understanding of the risks they face in the online environment. In addition to analyzing the situation with phishing, the article discusses preventive measures to protect citizens from such attacks. It provides practical insight into defense strategies, emphasizing both individual and collective efforts to improve cybersecurity resilience. The article is intended to provide readers with the knowledge necessary to recognize and mitigate potential threats. The findings and recommendations presented in this article serve as a valuable resource for individuals and businesses looking to strengthen their defenses against the ever-changing tactics used by online scammers.

Kalit so'zlar: *fishing hujumi, ijtimoiy muhandislik, zararli dasturga asoslangan fishing, fishing veb-saytlari, fisher, internet, aldamchi fishing, klon fishing*
Ключевые слова: *фишинговая атака, социальная инженерия, фишинг с использованием вредоносного ПО, фишинговые веб-сайты, фишер, Интернет, обманный фишинг, клон-фишинг.*
Key words*: phishing attack, social engineering, malware-based phishing, phishing websites, phisher, internet, deceptive phishing, clone phishing.*

INTRODUCTION

In recent years, the world has seen an active increase in cybercrime. Cybercriminals come up with new schemes and methods every day to achieve their goals. Due to their ability to manipulate human psychology, phishing and social engineering attacks continue to be effective among cyber-attacks. Around the world, these attacks are expected to become more sophisticated, targeted and convincing over the next year. According to published data from State Technical Service Joint-stock company of Kazakhstan, in 2022, more than 1200 applications were recorded and processed, and in 2023, 2160 information security incidents regarding phishing attacks [1,2]. Having analyzed the statistics on phishing attacks over the past two years, we can understand that the risk of phishing attacks is also relevant for our country. Phishing is the combination of the social engineering and technical methods. Phishing is defined as sending malicious emails that claim to be from reputable sources [3].

Previous literatures in the topic of the phishing attacks were analyzed, exist 3 components in the phishing attacks. They are medium, vector and technical approaches. The first component is medium, exists 3 mediums for the phishing attacks internet, voice and short messages. Nowadays most of the phishing attacks are through the internet as it gives a good opportunity for the hacker to an effectively realize it. The second component is vector. It is the place to distribute fake links and phishing messages. The vector for the internet is websites, social networks and corporate mails. The vector for the voice is phone calls, voice messages. The vector for the short messages is your phone number. The technical approaches for the phishing attacks divides into 2 categories which are social engineering and malware-based phishing attack. Social engineering exploits the emotions of users, particularly fear of losing something valuable, leading them to disclose personal information to the phisher. In malware-based phishing attacks, malicious programs are covertly installed to grant the phisher access to the user's computer [4].

TYPES OF PHISHING ATTACKS

Phishers use different types of the phishing attacks to realize their idea. In the below we will consider these types: algorithm-based phishing, deceptive phishing, URL phishing, host file poisoning, content-injection phishing, clone phishing, whaling, spear phishing [5]. In the next we will consider several of them with examples in Kazakhstan.

Deceptive phishing is a type of phishing attack where the attacker impersonates a legitimate entity or organization to deceive the victim into providing sensitive information, such as login credentials, personal details, or financial information. This is typically done through emails, text messages, or other forms of communication that appear to be from a trusted source, such as a bank, social media platform, or online service provider. The deceptive nature of these phishing attempts often involves using convincing logos and branding to trick the victim into believing the communication is authentic. Once the victim interacts with the phishing message or website, they are prompted to enter their sensitive information, which is then captured by the attacker [5]. This is one of the common types of phishing in the Kazakhstan. In the figure 1 given examples of the counterfeiting e-commerce and online-banking websites. Attackers created a fake website under the name Joint Stock Company «Halyk Savings Bank of Kazakhstan» and JSC National Company «KazMunayGas». They announce that there is supposedly an official program from the company and encourage users to invest with them. To apply for participation in this program, people fill out their data, in this way the attacker will receive your sensitive data.

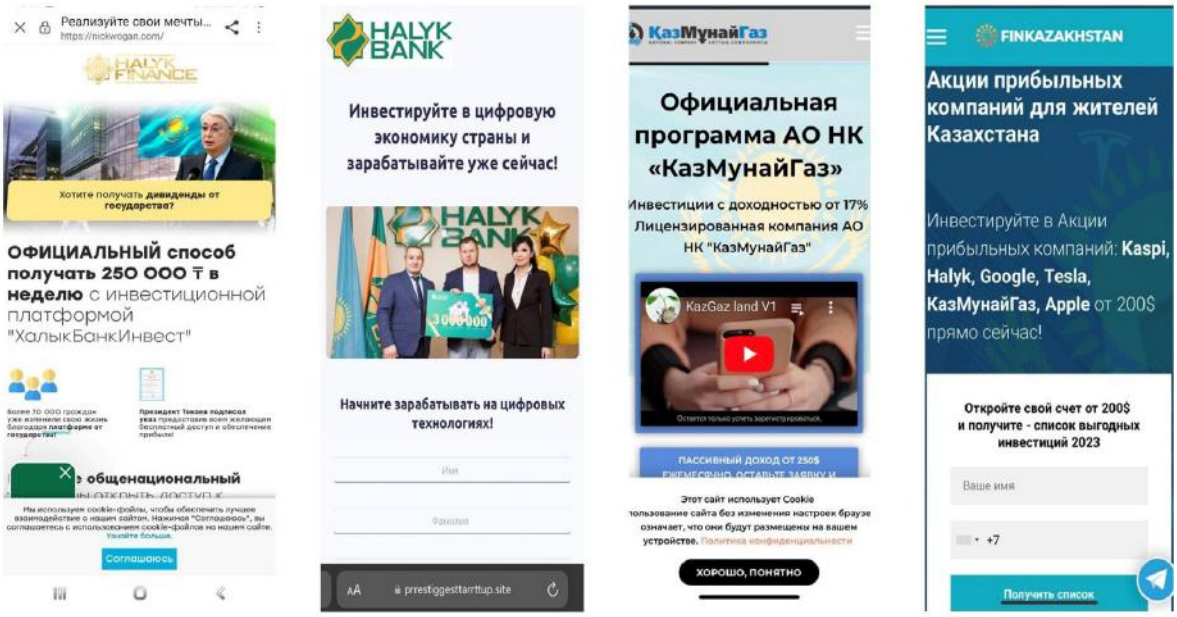

Figure 1. Deceptive phishing examples.

One more instance of the deceptive phishing which was distributed in our country shown in the figure 2. Fraudsters have created a website in the name of the non-existent Official Compensation Center, where they say that unpaid funds will be returned. They report that every citizen over 18 years of age has the right to receive payments for several years. During the instructions for a fictitious return, the author asks the viewer to indicate his data, bank card number, as well as a CVV/CVC code, through which pseudo-lawyers can take possession of your funds by debiting them from a bank card. The site uses the coat of arms and flag of Kazakhstan to instill trust with at first glance, and the interface is made as similar as possible to the interface of government websites in Kazakhstan to increase the level of trust in front of the victim.

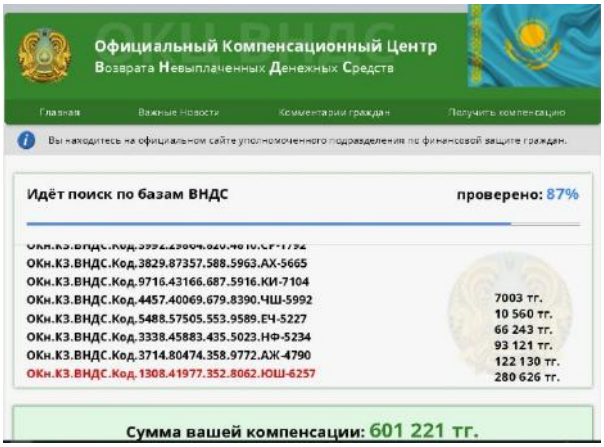

Figure 2. Deceptive phishing example.

Clone phishing is a type of phishing attack where the attacker creates a nearly identical replica, or "clone," of a legitimate email or website that the victim is familiar with. The attacker typically begins by obtaining a copy of a legitimate email that was previously sent to the victim, often by intercepting it or gaining access to the victim's inbox through previous phishing attacks or data breaches. Once the attacker has a copy of the legitimate email, they modify it slightly to include malicious links, attachments, or content. The modified email is then sent to the victim, who may be less suspicious of it because it appears to come from a trusted source they have interacted with before. Clone phishing relies on the trust that individuals have in familiar email senders or websites. Victims are more likely to interact with the cloned email or website because it closely resembles something they have previously encountered and trusted. However, by doing so, they

inadvertently provide sensitive information or credentials to the attacker, who can then exploit it for malicious purposes such as identity theft, financial fraud, or unauthorized access to accounts [6].

In the figure 3 have shown an example of the clone phishing with the website of the Joint Stock Company ««Otbasy bank» house construction savings bank». In the left-side the screen of fake website, in the right-side legitimate site. We can see that attackers copied full interface of the website. When you fill the fields your login and password will be send to the database of the attackers.

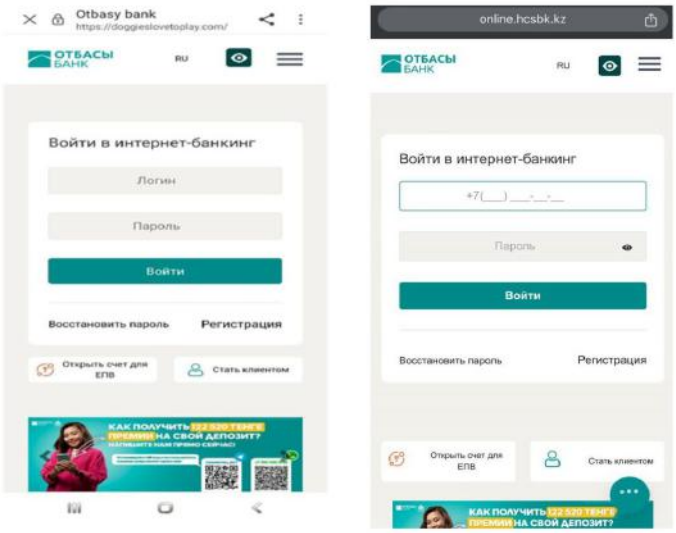

Figure 3. Clone phishing example.

In Kazakhstan, to sign a request for a government service, you must install NCALayer. In September 2023, hackers came up with a phishing Internet resource ncalayer.info/update.php, when opened, under the guise of an update for NCALayer, a malicious program like “Trojan Downloader" is downloaded and launched. After a chain of decryption and downloads that includes the popular GitHub code repository, the Venom RAT v6.0.1 malware is installed on the computer [7]. The peculiarity of this malicious program is that it has the functionality of a keylogger, stealing data, secretive remote computer control (VNC), and webcam control. As a result, the attacker can read information typed on the keyboard, view passwords, including from browsers, as well as install third-party applications.

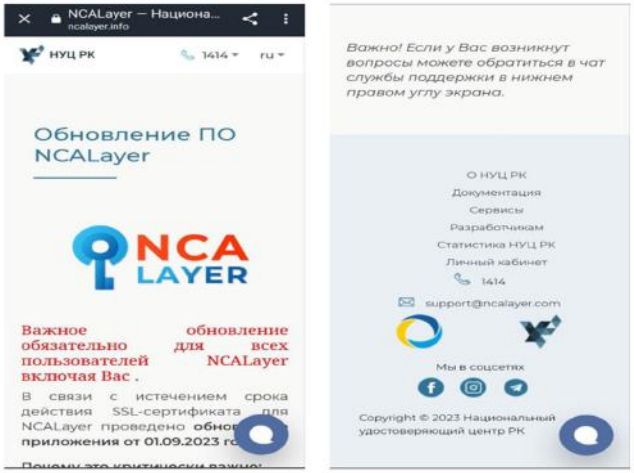

Figure 4. Example of the phishing attack with ransomware

Recommendations for preventing phishing

Fraudsters often distribute phishing sites through social media advertising, using a catchy headline or similar name from a well-known brand to attract as many people as possible. Always

carefully check the information that promises to transfer money to your bank account or bank card to receive your winnings. Banks do not engage in mass mailing of emails with attached files and links to access Internet banking system sites," warns Halyk Bank of Kazakhstan JSC. Let us recall that earlier the KZ-CERT service reported the discovery of five Internet resources disguised as homebank.kz KZ-CERT recommends taking special care when performing the following actions:

- Be suspicious of unsolicited phone calls, emails, especially links from people asking for employee data or other non-public information. If an unknown person claims to be from a trusted organization, then you should verify their identity directly with the company. Do not enter authentication data on dubious Internet resources.
- Beware of opening dubious links received in instant messengers and social networks. If you follow a link, you should pay attention to the domain name in the line where the address is written. Pay attention to the extra characters in the official name of the organization or Internet resource of the company conducting the campaign. Also look to the information on the site: fonts, grammatical errors, poor quality images, outdated design, excessive advertising and various links on the page. If when you click on links you are redirected to pages that are not similar to the official website, then this is a phishing resource.
- Pay attention to the information on the site: fonts, grammatical errors, poor quality images, outdated design, excessive advertising and various links on the page. If when you click on links you are redirected to pages that are not similar to the official website, then this is a phishing resource.
- Do not enter or store your personal data or bank card data. Do not share your three-digit CVV/CVC code (located on the back of your bank card) with anyone. Do not share the SMS code received from the bank. Do not share personal, confidential or corporate information about your organization unless you are sure the person has the authority to receive the information.
- Personal data, ID card details, bank card details, etc. b. Do not send copies of your documents containing personal data to anyone. Do not disclose personal or financial information via email. Do not send confidential information over the Internet unless you are sure of the legitimacy of the Internet resource.
- Banks never request logins, passwords, SMS codes and other confidential identification and personal data in letters or in any other way.
- If you are unsure whether an email or request is legitimate, you should verify it by contacting the company directly. However, do not use the contact information provided in the letter or via a link from the letter.

CONCLUSION

In conclusion, this article has provided a comprehensive exploration of the most prevalent phishing attacks targeting individuals in Kazakhstan, shedding light on the tactics employed by Internet scammers in the region. By dissecting these attacks, we have gained valuable insights into the evolving strategies that pose a threat to our citizens' online security. The research underscores the critical need for heightened awareness among the public regarding the specific phishing landscape in Kazakhstan. Understanding the nuances of these attacks is pivotal for individuals to recognize and thwart potential threats effectively. Moreover, this knowledge serves as a foundation for implementing targeted protective measures that can significantly enhance cybersecurity resilience at both the individual and collective levels. The proactive approach outlined in this article emphasizes the importance of education and empowerment. By arming citizens with information about the most popular phishing attacks in Kazakhstan, we enable them to make informed decisions, thereby reducing the likelihood of falling victim to cyber threats. Additionally, the suggested protective measures offer practical steps that individuals, businesses, and policymakers can take to fortify their defenses against Internet scammers. As the digital landscape continues to evolve, so too must our strategies for safeguarding against cyber threats. By addressing the specific challenges faced by citizens in Kazakhstan, this article contributes to the broader conversation on cybersecurity, providing a localized perspective that can inform tailored protective measures. In doing so, it is our hope that this research will play a role in fostering a more resilient and secure online environment for the citizens of Kazakhstan.

REFERENCE

1. State Technical Service Joint-stock company of Kazakhstan (2022). *Итоговый дайджест АО «ГТС» за 2022 год.* https://sts.kz/itogi-goda/

2. State Technical Service Joint-stock company of Kazakhstan (2023). *Итоговый дайджест АО «ГТС» за 2023 год.* https://sts.kz/itogi-goda/

3. Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future internet*, 12(10), 168. , https://doi.org/10.3390/fi12100168

4. Alam, M. N., Sarma, D., Lima, F. F., Saha, I., Ulfath, R.-E.-, & Hossain, S. (2020). Phishing Attacks Detection using Machine Learning Approach. 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT). https://doi.org/10.1109/icssit48917.2020.9214225

5. Huang, H., Tan, J., & Liu, L. (2009). Countermeasure Techniques for Deceptive Phishing Attack. 2009 International Conference on New Trends in Information and Service Science. https://doi.org/10.1109/niss.2009.80

6. Kumar, Mr & Gouda, Sandeepta. (2023). A comprehensive study of phishing attacks and their countermeasures. https://doi.org/10.13140/RG.2.2.36686.13120.

7. State Technical Service Joint-stock company of Kazakhstan (2023). *Технический разбор инцидента с фальшивым обновлением NCALayer.* https://sts.kz/2023/09/07/tehnicheskij-razbor-incidenta-s-falshivym-obnovleniem-ncalayer/