ELECTRONIC VICTIMS

Tukhtasinov Alyorbek
Student of Nurafshon branch of Tashkent University of Information Technologies (TUIT) named after Muhammad al-Khwarizmi
alyortuxtasinov2@gmail.com
Kuldoshev Otabek
Student of Nurafshon branch of Tashkent University of Information Technologies (TUIT) named after Muhammad al-Khwarizmi
kuldoshevotabek87@gmail.com
Raxmatullayeva Maftuna
Student of Nurafshon branch of Tashkent University of Information Technologies (TUIT) named after Muhammad al-Khwarizmi
Maftunaraxmatullayeva1112@gmail.com

Abstract. This article explores the phenomenon of phishing in the context of social engineering, a common form of cybercrime. Phishing involves deceptive methods used by "intelligence hackers" to encourage individuals to disclose confidential information or perform certain actions. The article explores the various manifestations of phishing attacks, their impact on victims, and the methods employed by cybercriminals. It highlights the importance of online security and provides practical advice on mitigating risks associated with phishing. The article concludes by emphasizing the need to raise awareness and vigilance to combat this growing threat.

Keywords. Phishing, social engineering, cybercrime, online security, e-fraud, email fraud, cybersecurity, personal data, theft of personal data, online fraud, internet fraud

With the rapid growth of internet and digital connecting, cybercrims have found new ways to exploit unwary individuals. One such method is phishing, which is a form of social engineering that tricks victims into disclosing sensitive information or takes actions that undermine their online safety. Phishing attacks have become increasingly sophisticated, making it difficult for users to identify fake attacks.

Phishing attacks are a form of cybercrime that uses social engineering techniques to deceive individuals and obtain valuable information or unauthorized access to their systems. These attacks rely primarily on psychological manipulation and use human vulnerabilities rather than technical weaknesses. Phishing attacks can occur through various channels such as emails, instant messaging, phone calls, or malicious websites. The goal is to convince victims to disclose confidential information or take actions that undermine their own security by assuring them that communication is legal.

Types of Fishing Attack

Phishing attacks each come in different forms with a specific approach and purpose. Some common species include:

- **Email Phishing:** One of the most common forms, this method involves sending false emails on behalf of financial institutions or prominent companies. These emails often contain urgent requests for personal information, such as passwords or credit card details.
- **Spear Phishing:** Unlike generic email phishing, spear phishing targets specific individuals or organizations. Cybercrime criminals conduct extensive research to tailor their posts and make them appear legitimate, increasing the chances of success.
- **Smishing:** This type of phishing happens via SMS messages. Attackers send text messages containing links or requests that lead to fake websites or give victims reason to disclose personal information.
- **Vishing:** Vishing, i.e., voice phishing, involves phone calls where attackers mimic legitimate organizations or individuals to trick victims into sharing sensitive information or making certain actions.
- **Farming:** Farming attacks run the Domain Name System (DNS) to target users to scam websites that mimic legitimate websites. Victims inadvertently enter their login information or financial information, which is then seized by the attacker. For example, www.PayPai.com can be submitted as www.PayPal.com. In this case, rarely users pay attention to the fact that the letter "l" has the letter "i" in its place. When contacting a link, www.PayPal.com will be visited on a site similar to a website, but forged, and the requested payment card information will be entered. The resulting information will quickly be in the hands of the hacker.

Impact on victims and organizations

Phishing attacks can also have dire consequences for individuals and organizations. Some significant effects include:

- **Financial loss:** Phishing attacks often aim to obtain sensitive financial information, such as credit card information or login information, which can lead to unauthorized transactions and financial losses for victims. According to THE U.S. Department of Homeland Security, theft of money from plastic cards and fraud are now among the most common crimes. By 2021, more than 2,700 dead were victims of Internet fraud.
- **Theft of personal data:** By deception, prompting victims to disclose confidential information, cybercrime criminals can access people's personal information and engage in fraud, such as opening an account through them or applying for a loan on behalf of the victim.

- **Data breach:** Phishing attacks can also target organizations with access to confidential information. This leads to data breaches, damage to customer data, trade secrets and other valuable assets.
- **Reputational damage:** Organizations that have been victims of phishing attacks can cause enormous damage to their reputations, which can undermine customer confidence and confidence in their ability to protect personal information. For example, according to the Regional Center for Processing, the official site interface for cybercriming from the Uzcard brand was downloaded and offered to enter a card number to receive bonuses. As a result, cybercriming was carried out in this way. Also, in 2021, 17,097,478 harmful and suspicious cases were identified in the address area of the national segment of the Internet, including 1,354,106 cyberattacks, according to the SUE “Cybersecurity center”. In accordance with Section 17 of the Criminal Code and Section 168 of the Criminal Code, section 17 and Section 168 of the Criminal Code, they face criminal charges for committing a crime of fraud using computer equipment.

Techniques used by cybercrimes

Cybercrimes use multiple techniques to make phishing attempts more reliable and successful. These include:

- **Fake websites and emails:** Attackers create fake websites or email templates similar to legitimate ones, making it difficult for victims to establish authenticity. As a clear example of this, one can get a phishing message that spread to eBay users in 2003. Accordingly, it was reported that users' accounts had been blocked and that credit card information should have been disqualified. These emails contained a link leading to a fake web page similar to the official website. The damage caused by this phishing attack was estimated at several hundred thousand dollars.
- **Social Engineering:** Phishing attacks rely on great mental manipulation, using human emotions such as fear, urgency, curiosity or confidence to get the desired response of the victims. One of the most famous social injners in history is Kevin Mitnik. Not only is he a world-renowned computer hacker and security expert, he is also the author of many books on computer security based on social engineering. In his opinion, it is easier to get a password through deception than to hack the security system.
- **Malware and Exploits:** Phishing attacks can involve the use of malware or exploits that infect users' devices or disrupt security systems. In this method of social injunction, the hacker uses data stores with a special malware. To do this, it leaves malware storage facilities near the victim's work environment, in public places and in hakazo locations. The abandoned storage facilities may have been downloaded by the hacker to the corporate logo and the official website address. On the surface of this disc can also be labeled "Executive Salaries". As a result, the victim who

seizes this storage unit will put it on his computer. This means that the attackers have reached their goal.

Reducing the risk of phishing

To protect against phishing attacks, individuals and organizations must adopt various preventive measures, including:

- **Awareness and Training:** Raising awareness of phishing methods and conducting training to identify suspicious emails, links or messages can significantly reduce the likelihood of being the victim of phishing attacks.
- **Email Filters and Anti-Phishing Software:** Running robust email filters and anti-phishing software can help identify and block phishing attempts before hackers achieve their goals.
- **Two-Factor Authentication:** Performing two-factor authentication creates an additional layer of security by requiring users to provide additional control, such as a unique code sent to their mobile devices when accessing accounts or accessing confidential information.
- **Secure password practices:** promoting the use of powerful, unique passwords and regularly updating them can reduce the risk of unauthorized access to personal or organizational accounts.
- **Check requests:** when receiving confidential information or requests for financial transactions, individuals must independently verify the legitimacy of the request through trusted channels, such as directly contacting the organization.

Despite being blind, brothers Mundir, Mushid and Shadi Badir were able to carry out several large-scale fraud schemes in Israel in the 1990s using social engineering and voice falsification techniques. In a TV interview, they say: "**Only those who do not use phones, electrical and laptops are safe on the network**". In fact, despite efforts to combat phishing attacks, cybercrimes continue to develop their methods and pose constant challenges for individuals and organizations. As technology advances, attackers will find new ways to exploit vulnerabilities and manipulate unsuspecting victims. The fight against phishing requires a versatile approach that combines technological solutions, user awareness and regulatory measures to create a safer online environment.

Conclusions

Phishing attacks in the field of social engineering have emerged as a significant threat to online security. The increasing sophistication of these attacks requires cybercriminals seeking to exploit vulnerable individuals to raise awareness and take proactive measures to protect them. They can take steps to strengthen their defenses by understanding different types of phishing attacks, their impact on victims and organizations, and the methods employed by cybercriminals, individuals and organizations. Through a combination of user training, robust security measures, and

continued vigilance, we can minimize the risks associated with phishing and create a safer digital landscape for everyone.

References:

1. Tahirov, B.N. (2022). Basics of Information Security. Educational application. https://uniwork.buxdu.uz/resurs/13241_2_62D59433227506AEF1BEA6CA35C85C6376F78A92.pdf
2. Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking. https://theswissbay.ch/pdf/Books/Computer%20science/socialengineering_thescienceofhumanhacking_2ndedition.pdf
3. **Lex Uz** — is a national database of legal documents of Uzbekistan on the Internet.
4. Criminal Code of the Republic of Uzbekistan - https://lex.uz/docs/-111453?ONDATE2=14.03.2022&action=compare
5. Ganiyev, S.K. (2020). Basics of Cybersecurity. Educational application.
6. Kun.uz — is a news website. https://kun.uz/uz/news/2021/06/18/ozbekistonda-qaysi-turdagi-kiberhujumlar-keng-tarqalgani-haqida-malumot-berildi?q=%2Fuz%2Fnews%2F2021%2F06%2F18%2Fozbekistonda-qaysi-turdagi-kiberhujumlar-keng-tarqalgani-haqida-malumot-berildi
7. A. Akerlof, J. Shiller (2015). Phishing for Phools: The Economics of Manipulation and Deception. https://www.goodreads.com/author/show/1404728.George_A_Akerlof