37. PHISHING IN SOCIAL ENGINEERING

Betenya K.S.

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Subbotkina I.G. – Associate Professor

This paper examines phishing as a serious threat in the online environment. It has the potential to cause a significant damage to the Internet users. Given methods necessary for the safe usage of social networks are considered.

One of the main and dangerous forms of social engineering is phishing. Phishing is a type of online fraud aimed at obtaining confidential data. This problem is getting more dangerous every day due to the insane pace of the Internet development and technologies.

There are different forms and ways of deceiving Internet data. These forms are constantly being upgraded and adjusted to current trends. Even a knowledgeable person can be attacked by hackers. The most common type of an attack is a malicious email or message on a social network. By clicking on this message, user disclose personal data to an attacker. Any common reason for disclosing confidential data is the method of blackmail, threats or delusion of a potential victim. By lulling vigilance, user reveal personal information and attacker has a great chance to steal data.

Frequent Internet users are aware of the basic techniques of scammers and have a higher degree of security. But not everyone has rich experience of using the Internet, so such people are in a potentially dangerous. Some people are particularly at risk due to their inexperience in using the Internet and difficulties with the interface.

Any information about the loss or stolen accounts on social networks, confirms – this case always happens when user serfs on the Internet with a help of malicious link. A common situation of losing an account is receiving a link in private messages. This is due to the fact that a sender of this message was hacked in order to send a malicious link to all users who have ever interacted with the victim. Clicking on a malicious link identifies the user as a victim who will also send malicious links to other users. A guarantee of security in such cases to clarify the status of the sender's account.

A resource such as a browser is the main source of knowledge and information. In most cases, mostly using websites, user need to provide some personal information or agree to get cookie files [1]. Attackers may get interested in detail information. In this regard, every user of the global network is obliged to monitor the domains of the sites. One of the most popular techniques of detractors is to change the domain of a popular site by one character so that an ordinary user does not notice it. As a result, the difference will not be noticeable and users will visit the attacker's site. It is also a user's responsibility to use the sites with additional "https" encryption [2], and not with simple ‘http'.

Users need to install Two-Factor Authentication (2FA) [3] and Zero-Trust Network Access (ZENA) in a personal account. In this case the probability of stealing data is significantly reduced. Updating antivirus systems, email filters, and firewalls is also a necessary regular procedure. Every user of the web needs to be vigilant when using a network. By observing such basic techniques, a user protect himself from all kinds of attacks.

It is important to stress that phishing is a very flexible and dangerous structure that affects everyone. It is extremely important to be careful and vigilant when using the Internet in different cases. Hackers can use personal data for their own purposes. This leads to the loss of funds and accounts. Users should be aware of the typical signs of phishing attacks, such as a suspicious request for personal information or emails with spelling errors. When using websites, user should be careful with the site domains and do not enter personal data on questionable sites. By being vigilant and applying basic security measures, users can reduce the risk of becoming a victim of phishing and protect funds and accounts.

References:

1.Cookie stealing in WordPress: Understanding the Risks and Consequences. Karishma Sundaram. [Electronic resource]. – Mode of access: https://www.malcare.com/blog/cookie-stealing/. Date of access: 22.02.2024.

2.What is HTTPS and Why is it important. Avery Jones. [Electronic resource]. – Mode of access: https://wavebrowser.medium.com/what-is-https-and-why-is-it-important-85cd170cee71. Date of access: 01.03.2024.

3.The Importance of Two-Factor Authentication. Microsoft Corporation. [Electronic resource]. – Mode of access: https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/importance-of-two-factor-authentication. Date of access: 12.03.2024.