UDC 343.9

PHISHING AS ONE OF THE RELEVANT TYPES ONLINE FRAUDS

Rozhneva E.M., PhD, Associate Professor,
Mamontov A.A., student of the group IBs-251, I course
T.F. Gorbachev Kuzbass State Technical University,
Kemerovo

Every year, millions of users become victims of phishing, one of the most common types of online fraud in the modern digital world. The purpose of the study is to analyze phishing and identify ways to counter this type of online fraud. There are some tasks to solve:

1. define the term phishing and describe the history of its origin;
2. consider the types of phishing attacks;
3. learn how to combat phishing;
4. develop a questionnaire and conduct a survey among Internet users of different age categories in order to determine the level of awareness of users about this type of Online fraud (phishing), as well as their willingness to counter such threats.;
5. analyze the data obtained and draw a conclusion;

The relevance of the article is due to several factors:

1. The article highlights one of the most pressing problems of modern cybersecurity.
2. It provides a comprehensive understanding of the types and methods of phishing.
3. It offers practical protection recommendations.
4. It serves as the basis for educational programs and the development of new anti-phishing technologies.
5. Helps to predict future threats and prepare for them in advance.

Research methods: the analysis of literature and the Internet resources on this issue, survey of respondents using google-forms.

The practical significance obtained on the basis of the conducted survey may further consist in:

1. Increase user awareness.
2. Recommendations on personal data protection.
3. Security tools for organizations.
4. Databases for educational programs.
5. Data for the development of security technologies.
6. The basis for further research.
7. Practical cases for analysis.

The theoretical significance of the study is represented by the following positions:

1. Systematization of knowledge about phishing.
2. Classification of phishing types.
3. Analysis of social engineering methods.
4. Overview of the technical aspects of threats.
5. Statistical and economic data.
6. Historical context.

To begin with, we consider it advisable to define the term “phishing” under consideration. This is a type of online fraud aimed at gaining access to confidential user data – logins and passwords. This is achieved by sending mass emails on behalf of popular brands, as well as personal messages within various services, for example, on behalf of banks or within social networks. The email often contains a direct link to a website that looks indistinguishable from the real one, or to a website with a redirect. After a user lands on a fake page, fraudsters use various psychological techniques to induce the user to enter their username and password on the fake page, which they use to access a specific site, which allows fraudsters to gain access to accounts and bank accounts. The phishing technique was described in detail in 1987, and the term itself appeared on January 2, 1996 in the Usenet newsgroup, although it may have been mentioned earlier in the hacker magazine 2600.

To solve the second problem, let’ turn to the types of phishing attacks:

- Social engineering: a person always reacts to events that are important to him. Therefore, phishers try to alarm the user with their actions and cause his immediate reaction. Therefore, for example, an email with the headline “to restore access to your bank account ...”, as a rule, attracts attention and forces a person to follow a web link for more detailed information.
- Web links: Most phishing methods are limited to disguising fake links to phishing sites as links from real organizations. Addresses with typos or sub-domains are often used by scammers.

For example, https://www.yourbank.example.com / looks like Yourbank’s address, but in fact it links to a phishing part of the site example.com . Another common trick is to use outwardly correct links that actually lead to a phishing site. For example, https://ru.wikipedia.org/wiki / The truth will lead not to the “Truth” article, but to the “Lie” article.

One of the old methods of deception is to use links containing the “@” symbol, which is used to include a username and password in the link. For example, the link http://www.google.com@members.tripod.com / will not lead to www.google.com , and on members.tripod.com on behalf of the user www.google.com . This functionality has been disabled in Internet Explorer, and Mozilla Firefox and Opera issue a warning and offer to confirm access to the site.

Another problem was found when browsers processed International Domain Names: addresses visually identical to the official ones could lead to fraud sites.

- Bypassing filters: Phishers often use images instead of text, which makes it difficult for anti-phishing filters to detect fraudulent emails. But experts have learned how to deal with this type of phishing. For example, mail filters can automatically block images sent from addresses that are not in the address book. In addition, technologies have emerged that can process and compare images with the signatures of similar images used for spam and phishing.
- Websites: The deception does not end with the victim visiting a phishing site. Some phishers use JavaScript to change the address bar. This is achieved either by placing an image with a fake URL on top of the address bar, or by closing the real address bar and opening a new one with a fake URL.

An attacker can exploit vulnerabilities in the scripts of a genuine website. This type of fraud (known as cross-site scripting) is the most dangerous, as the user logs in to the real page of the official website, where everything (from the web address to the certificates) looks authentic. Such phishing is very difficult to detect without special skills. This method was applied to PayPal in 2006.

To counter anti-phishing scanners, phishers began using Flash-based websites. Externally, such a site looks like a real one, but the text is hidden in multimedia objects.

- Malicious phone apps: Smartphone apps are also used for phishing. There are some kinds:
    - The application prompts the user to enter the bank card data, after which this data becomes known to intruders
    - A Trojan application establishes access to data on the phone, some scammers may additionally change calls or pose as an employer in order to install the application
    - The application requests permission and conducts the sending of paid SMS messages or calls
    - The application collects information about the device's location, status, and file storage
    - The application is pre-installed on the phone, performs self-download, shows ads
    - In addition, legal banking applications are vulnerable to fraudsters.
- New threats:Today, phishing goes beyond online fraud, and fake websites have become just one of its many areas. Emails that are allegedly sent from a bank may inform users about the need to call a specific number to resolve problems with their bank accounts. This technique is called vishing (voice phishing). By calling the specified number, the user hears the instructions of the answering machine, which indicate the need to enter his account number and PIN code. In addition, hackers can call victims themselves, convincing them that they are communicating with representatives of

official organizations using fake numbers. Most often, attackers pose as employees of the bank's security service and inform the victim about a recorded attempt to illegally debit funds from his account. Eventually, the person will also be asked to provide their credentials.

SMS phishing, also known as smishing (from “SMS” and “phishing”), is also gaining momentum. Fraudsters send out messages containing a link to a phishing site. By logging in and entering their personal data, the victim transmits them to the attackers in the same way. The message may also talk about the need to call the scammers at a specific number to resolve "problems that have arisen."

To solve the next problem, we will study methods to combat phishing:

1. User education: One of the methods of combating phishing is to teach people how to distinguish and combat phishing. People can reduce the threat of phishing by slightly changing their behavior. For example, in response to a letter requesting “confirmation” of an account (or any other common request from users), experts advise contacting the company on whose behalf the message was sent to verify its authenticity. In addition, experts recommend entering the organization's web address into the browser’ address bar yourself instead of using any hyperlinks in a suspicious message.

Almost all genuine messages from organizations contain references to certain information that is inaccessible to phishers. Some, such as PayPal, always address their recipients by name, and an email with the general message “Dear PayPal customer” may be regarded as a phishing attempt. Letters from banks and credit institutions often contain part of the account number. However, recent research has shown that people do not distinguish between the appearance of the first digits of an invoice or the last digits, while the first digits may be the same for all clients of a financial institution. It can be explained to people that any letters that do not contain any specific personal information are suspicious. But the phishing attacks of early 2006 contained such personal information, therefore, the presence of such information does not guarantee the security of the message. In addition, according to the results of another study, it was found that the presence of personal information does not significantly change the percentage of success of phishing attacks, which indicates that most people do not pay attention to such details at all.

The anti-phishing working group believes that conventional phishing methods will soon become obsolete as people become more aware of the social engineering used by phishers. Experts believe that in the future, pharming and various malware will be more common methods of information theft.

2. Technical methods:

- Phishing threat warning browsers: Another way to combat phishing is to create a list of phishing sites and then check against it. A similar system exists in Internet Explorer, Mozilla Firefox, Google Chrome, Safari and Opera browsers. Firefox uses Google’s anti-

phishing system. Opera uses PhishTank and GeoTrust blacklists and GeoTrust exclusion lists. According to the results of an independent 2006 study, Firefox was found to be more effective in detecting phishing sites than Internet Explorer.

In 2006, a technique was introduced for using special DNS services that filter known phishing addresses: this method works with any browser and is close to using the hosts file to block ads.

- Complicating the authorization procedure: The Bank of America website prompts users to select a personal image and displays this user-selected image with each password entry form. And users of banking services should enter a password only when they see the selected image. However, a recent study has shown that the absence of an image does not stop most users from entering a password.
- Combating phishing in emails: Specialized spam filters can reduce the number of phishing emails received by users. This technique is based on machine learning and natural language processing when analyzing phishing emails.
- Monitoring services: Some companies offer round-the-clock monitoring, analysis, and assistance in shutting down phishing sites to banks and other organizations potentially exposed to phishing attacks. Individuals can help such groups by reporting phishing cases. [3]

3. Antivirus software:

- Kaspersky: Web Threat Protection checks links for phishing web addresses. This avoids phishing attacks. A particular example of phishing attacks is an email message purporting to be from a bank of which you are a client, with a link to the bank’s official website on the Internet. Using the link, you get to an exact copy of the bank's website and can even see its web address in the browser, but you are on a fictitious website. All your further actions on the website are monitored and can be used to steal your funds.

Since a link to a phishing website can be found not only in an email message, but also, for example, in a messenger message, the Web Threat Protection component detects attempts to access a phishing website at the web traffic verification level and blocks access to such websites. Lists of phishing web addresses are included in the Kaspersky Endpoint Security package. [4]

- Dr.Web: provides real-time web page verification, blocks phishing Internet resources, and prohibits access to non-recommended and potentially dangerous sites. [1]
- Avast: Helps protect millions of people from online fraud, malware, and phishing through the implementation of Scam Guardian Pro, a set of tools designed to protect users at all stages of online interaction.

Scam Guardian Pro offers a multi-layered approach to fraud prevention. It combines:

- Avast Assistant, which uses artificial intelligence for natural language processing, helps users navigate potential threats, analyzes suspicious emails or links, and provides clear recommendations when something seems suspicious.
- Web Guard is a tool that scans the content and code of a website in real time, blocking hidden malware, malicious scripts and fake web pages before they are loaded.
- Email Guard, which uses contextual AI to mark emails as safe or unsafe, helps users instantly recognize phishing attempts on different devices and in different browsers [2].

To solve the remaining tasks, let's turn to the results of the survey:

The survey was attended by students of the Vocational School, students of KuzSTU and other respondents of different age categories. The questions were aimed at determining the level of awareness about phishing and skills to protect against it.

The questions in the questionnaire were as follows:

- How old are you?
- Do you know what phishing is?
- How often do you receive suspicious emails or co-communications that may be phishing?
- What signs of a phishing email/message can you name?
- What do you usually do when you receive a suspicious email or message?
- Have you ever used services to check suspicious links or emails?
- Do you think you have enough knowledge to protect against phishing?
- Which source of information about phishing do you consider the most useful?

A total of 86 questionnaires were analyzed, among them: 51.2% of respondents belong to the age group of 16-18 years, 35 people aged 19-23 years, and the remaining 8.2% of respondents are people over 30 years old. 36 people replied that they knew well what phishing was, which was 41.9%. Respondents who do not know anything about him made up 16.3% of the respondents, while the remaining 41.9% indicated the option "I have heard, but I cannot clearly define".

The respondents were asked how often they receive suspicious emails or messages that may be phishing. 42 people (48.8%) replied that they receive such messages once a month, 10.5% of respondents – once a week or more often, the remaining 40.7% of the survey participants have never or almost never received such messages.

Regarding the question of the signs of a phishing message, the most common were: a link to a strange or unfamiliar website (80.2%), a suspicious or unfamiliar sender's address (77.9%), please provide personal information (69.8%). Respond-

ents are less likely to consider the urgent requirement to perform an action and typos in the text as signs of a phishing email.

Among the students who answered the question about actions when receiving a suspicious email or message, 67.4% immediately delete it, 29.1% and 33.7% chose the options “I open to check, but I don’t click anything” and “I inform the support service or block the sender”, respectively. Only 4 people (4.7%) follow the links to sort out what is happening.

The majority of Students (40.7%) who answered the question “have you ever used services to check suspicious links or emails?” indicated that they do not use them and do not consider it necessary, while the other part of respondents (30.2%) have never used such services, but would like to try. The remaining 25 respondents (29%) replied that they used such resources sometimes or regularly.

Regarding the question of having sufficient knowledge to protect against phishing, the majority (52.3%) answered that they can resist this type of fraud, but sometimes they doubt it, 33.7% are confident in their abilities to recognize phishing. 12 people out of the respondents (13.9%) consider their knowledge in this field insufficient.

Regarding the issue of the source of information about phishing, the official websites of government agencies and banks, as well as articles and blogs on cybersecurity, are considered the most useful. That’s exactly what 37.2% and 31.4% of respondents answered, respectively. Respondents consider training courses or webinars (3.5%), advice from friends and acquaintances (8.1%), as well as social networks and messengers (15.1%) to be the least useful sources.

Thus, despite the relatively high awareness of the basic signs of phishing, a significant part of the respondents demonstrate gaps in knowledge, lack of confidence in actions and a low level of use of additional protection tools. This makes them vulnerable to online scams.

Список литературы:

1. https://cryptostore.ru/catalog/antivirus-dr-web-security-space-windows-mac-linux
2. https://finance.yahoo.com/news/avast-helps-protect-millions-online-031200615.html
3. https://ru.wikipedia.org/wiki/Фишинг
4. https://support.kaspersky.ru/kes11/128018