УДК 004.056.53=111

ANALYSIS OF THE MAIN PHISHING THREATS AND DESTRUCTIVE CONSEQUENCES

Tereshchenko V., 21КН **e-mail: viacheslaw.tereshcchenko@gmail.com**
Zaitseva N.V., language adviser **e-mail: nataliia.zaitseva@tsatu.edu.ua**
Tavria State Agrotechnological University

This article discusses one of the most common types of online fraud –phishing. The main consequences of phishing attacks are considered and different protection methods are analyzed.

У даній статті розглядається один з найпоширеніших видів Інтернет-шахрайства – фішинг. Розглянуто основні наслідки фішинг-атак та проаналізовано різні методи захисту.

Problem setting. If the user believes that the mailbox is secure, they should remember that there is a new form of junk mail. This type of junk mail is not only unexpected and annoying, but also facilitates the theft of passwords, credit card numbers, account information and significant private information. This article is devoted to this technique, called phishing. Phishing is a serious problem for both ordinary users and global companies. And the scale of the problem continues to grow. According to the *Anti-Phishing workgroup*, the number of phishing attacks increases by 50 percent every month. Thus, banks and agencies do not know how to stop this new fraud, since the attack is aimed at human psychology, and recommendations to ignore this type of electronic messages are ineffective.

Analysis of recent research and publications. According to the results of the first wave of social research conducted by the *EMA Association* and *Gemius Ukraine* in autumn 2016, 12% of the respondents personally faced fraud with payment cards (that means that they were deceived and / or robbed by scammers). But while 65% of the respondents were ready to use new, unknown websites for remittances. Any of these online resources may turn out to be phishing [1].

Google employees conducted a research that focused on sales of online accounts on the black market. They found that the most common reason for personal data leakage was phishing. The results of this study were presented at the Computer and Communication Security conference in Dallas [2]. It turned out that 15% of all users at least once confronted scammers on the network, and lost their account information and even information on payment cards.

The purpose of this paper is to study the criminal concept, and to enlist what needs to be done in order not to become a fishing victim.

Basic material research. Phishing is a form of fraud designed to deceive the user; scammers pretend to be entrepreneurs, private companies or financial organizations (public or private entities that may have some access to financial data) to obtain confidential data such as access codes, credit card information, e-mail and others. Typically, phishing is based on fraudulent links that invite a user to enter their data on a fake site.

So, let’s learn how phishing works. Phishing technology is sending millions of false messages that seem to come from recognized or trusted websites, like a user’s bank or a prominent company. As messages and websites seem official, they can deceive many people, considering them legitimate. People usually respond to these email inquiries with their credit card numbers, financial state or account information or delicate personal information. To make these messages seem even more real, the cheater usually includes a false link that appears to lead to an allegedly legitimate website, but actually leads to some fake site or a pop-up window created by a scammer which looks exactly like an official website. These copies are called *pirate sites*. A user enters personal information on one of these websites, not knowing that it will be transferred directly to the creative scammer. The main destructive consequences of inattentive usage of websites and emails are:

- access to confidential users’ information – logins and passwords;

- registration information theft;
- stealing of clients' information and electronic payment system data of a bank [3].

In a phishing attack, an attacker uses social engineering to convince a user to click on a link or download software that then steals passwords, or can lead to chaos in other ways. So, if an Internet-user clicked on the link to an unknown site, and what could be worse, entered confidential information, this could result in the password stealing for accessing the bank account, the subscription to paid SMS messages and various content services, the account theft in social networks and getting e-mail addresses from the contact book for spamming.

Unfortunately, there are no technical tools or software that can be used to prevent phishing. The best defense is to educate yourself and other users to make them think carefully before clicking a link or accepting a download, even if they appear to come from a legal source.

Since phishing is a method for sending bulk messages to multiple users, you can receive emails from companies whose clients you do not represent, in which such information is also requested. In these cases, directly, discard them.

So, when an e-mail is in your inbox take following actions:

- If the web address is not familiar to you, assume that this might be a phishing attack.
- You need in the first place to check the URL of a suspicious site.
- Avoid referring to links that come by email like invitations in social networks.
- Decline filling out forms in emails that request personal financial information.
- Make sure that the URL in the browser address bar starts with *https: //* to make sure that you are connecting to a secure web server. Access the address directly in the browser bar, not through links.
- When an organization refers to its users, it usually does this individually. Either a bank or any other respected organization turns to a customer by name. If there is a general salutation, for example, "Dear User", a client should suspect that this is phishing.
- Use secure sites. When organizations request any confidential information, they often use definite secure technologies (the commonly used technology nowadays is SSL) to make sure that no one can intercept the data and no one becomes a fraud object.

There are also some general recommendations on routine Internet surfing:

- No serious financial institution will ask a client about a card number, PIN or password either by e-mail, by phone or in any other way.
- Change the password periodically and use difficult passwords. Passwords like '*12345678*', '*qazxsw*' are the most widely-known and commonly used. Use combinations of numbers, letters and special symbols.
- Do not use the same password for multiple websites.
- Users should have a secure and updated antivirus software or scanner [4].

Conclusion. Over the past 20 years, the Internet is a full part of our lives. We use electronic payment services, pay utility bills with the help of Internet banking, conduct business and friendly correspondence. If a person does not follow the basic rules of caution their confidential information can become a prey to scammers.

References

1. Фишинг - главная причина утечки персональных данных [Електронний ресурс]. – Режим доступу: https://marketer.ua/fishing-golovna-prichina-kradizhki-personalnih-danih
2. Фишинг в 2017 году [Електронний ресурс]. – Режим доступу: https://ema.com.ua/phishing-statistics-results-2017
3. Wikipedia, 'Phishing' [Електронний ресурс]. – Режим доступу: http://en.wikipedia.org/wiki/Phishing
4. Microsoft support, 'Identify fraudulent e-mail and phishing schemes' [Електронний ресурс]. – Режим доступу: http://office.microsoft.com/en-us/outlook-help/identify-fraudulent-e-mail-and-phishing-schemes-HA001140002.aspx