УДК 004.056.53=111

METHODS FOR RECOGNITION AND AVOIDING SOCIAL ENGINEERING ATTACKS

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

The article is devoted to the psychological manipulation technique, which is often used in order to induce a person to perform certain actions or to disclose confidential information, and to the methods of protection against it.

Статтю присвячено психологічній маніпулятивній техніці, яку часто використовують з метою спонукати людину виконати певні дії чи розголосити конфіденційну інформацію, та основним методам захисту від неї.

Problem setting. It's been around for ages to deceive unsuspecting people in order to deprive them of money or information. Thieves hunt for such people almost from the very beginning of civilization. Though the same is true today, in the modern era of technology, people can still be deceived, but it has the potential to prove that it is more lucrative to deprive users of their private information online.

Analysis of recent research and publications. According to Chris Hadnagi [1], social engineering is a form of techniques used by cybercriminals designed to attract unsuspecting users to send their confidential data, infecting their computers with malware or by opening links to infected sites. Technical director of *SSR (Symantec Security Response)* Kevin Mitnick asserts that scammers do not usually try to use technical vulnerabilities in the operating system – they follow a person. There is no need to have so much technical skill to find an Internet user at the moment of his weakness who might want to see an attachment containing malicious contents. Only about 3% of the malicious applications people are facing are trying to exploit the technical faults. The other 97% try to deceive users through one of the type of social engineering scheme.

The purpose of the paper. This study is an attempt to analyze the criminal concept and to enlist recommendations on what needs to be done to avoid becoming a victim.

Basic research of materials. Social engineering is a real problem for any company and Internet user security. Social engineering is more dangerous than hacking, because it depends on human errors, not vulnerabilities in software and operating systems. Hence errors made by legitimate users are much less predictable it is much more difficult to detect and to prevent them than to avert a malicious program intrusion.

What does social engineering look like in practical situations? It can stand out as an email that was designed to look like a message from a reliable organization, for example, your messaging service or even from your bank. But if you open it and click on the attachment you can install a malware or a ransom. Or it may be disguised to look like it comes from someone inside your organization (for example, such as *IT@myorganization*), someone whose computer is easily compromised. The rule is – to think before click.

Once social engineers have a target, they usually start an attack, collecting public information about their victims. Many social engineers are gradually acquiring information over time, so they do not arouse any suspicion. To stop obvious collection of private information is a clue when protecting against social engineering.

How to protect yourself from social engineer attack:

- Slow down. Spammers want you to act first and think later. If the message conveys a sense of urgency or uses high-pressure sales tactics, be skeptical; never allow their urgency to influence your thorough review.

- Study the facts. Be dubious of all unwanted messages. If the email is similar to the company you are using, do your own investigation. Use the search engine to go to the site of a real company or telephone directory to find your phone number.
- Turn down requests for assistance or help. Legal companies and organizations will not contact you for assistance.
- Deepening e-mail is unchecked. Spammers, hackers and social engineers who control people's e-mail accounts (and other accounts) have become uncontrollable. Once they control somebody's account, they hunt for trust of every person's contact.
- Beware of any downloads. If you personally do not know the sender and expect a file from them, downloading something is an error. Even when the sender turns out to be someone you know, check links or attachments with a sender in person before opening links or downloading files.
- Protect your devices. Install email filters, firewalls, antivirus software and save the updates.

Conclusion. Social engineering is a technique that has emerged from sociology and claims to be the totality of the knowledge that guides, streamlines and optimizes the process of creating, modernizing and reproducing new ('artificial') social realities. In a certain way, it 'completes' sociological science, concludes it at the stage of transforming scientific knowledge into models, projects and constructions of social institutions, values, norms, activity algorithms, relations, behavior, etc. Despite the fact that social engineering is a relatively young science, it causes a great damage to the society processes.

References

1. Spam and phishing in 2017 [Електронний ресурс]. – Режимд оступу: https://securelist.com/spam-and-phishing-in-q1-2017/78221
2. How social engineers seek information for hacks [Електронний ресурс]. – Режим доступу: http://www.dummies.com/ programming /networking /how-social-engineers-seek-information-for-hacks
3. Wikipedia, 'Social engineering' [Електронний ресурс]. – Режим доступу: https://wikipedia.org/wiki/Social_engineering
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