**Oleg Romaniuk**
Kyiv National University of Technologies and Design
(Kyiv)
Scientific supervisor – PhD Maria Chernets

## SOCIAL ENGINEERING

The term Social engineering, the method of receiving necessary access to information based on features of human psychology is well known for a long time. A main objective of social engineering is gaining access to confidential information, passwords, bank data and other protected systems. Swindlers always used psychological methods of impact on the person, and a digital era presented new opportunities for swindlers [1].

In the 21st century it is difficult to find the person who does not use social networks, messengers, online banks and other popular industries of the global Internet. The usual password from your social network, is access to your private messages, working mail or to other personal information, and the fingerprint allows to make financial transactions from your bank accounts. Theme Social engineering is relevant today and is necessary for acquaintance the modern man of the 21st century. The specialist in IT safety and the outstanding cryptology Bruce Schneider, says that the mathematics in respect of safety is faultless, and computers and people are vulnerable. Computers are vulnerable to software attacks, and people are psychologically affected. Indeed, a person is the weakest link in any system of protection, it's easy to "break", playing on emotions and weaknesses.

Techniques of social engineers are different, but one of the main methods is cognitive distortion, which is the use of human inattention and negligence to trifles. Phishing is the most widespread way of fraud in network. Every year with the help of phishing stealing 45 million dollars. Observance of elementary rules of cyber security saves, but nevertheless even the trained people come across tricks of swindlers. The most trivial example of replacing a real web site (or a payment method) with a fake, a web site looks externally real and does not suspect that people make any payments

(product / service), but in fact the money goes to a fraudster. Still popular is the use of Trojan viruses, as well as infected smartphone applications downloaded from unreliable sources, USB flash drives, so that fraudsters can gain access to the victim's confidential information and financial accounts. Spyware gets a list of contacts, scheduled meetings and email correspondence, all in order for fraudsters to play a full-fledged presentation to the victim. If, in the case of the usual phishing, the victim simply uses a non-real website or a payment method (goods / services), then in the case of collecting information about the victim, the most realistic social engineering enters. Pretexting - when the fraudster collects information about the victims and their surroundings in advance, then even the smallest details - the pet's nickname, apartment number or hometown name are important in order to appear familiar to you. For example, in 2015, fraudsters, on behalf of the director of Ubiquiti Networks, demanded that their subordinates transfer $ 40 million, and the employees did. Psychologists have proven that under pressure from the authorities we can do a lot. According to the results of the experiment, 95% of nurses will inject a lethal dose of a drug to the patient without question, if it is prescribed by a doctor [2].

Reverse engineering implies that the victim herself turns to the scammer, the principle of Quid pro quo, since mutual services come into force here, the victim is ready to go even for minor offenses. In cybersecurity competitions, one of the tasks was "What can be done with the computer of the departed employee, in order to later gain access to the entire network. The simplest solution was to attach a sticker with a false technical support number, because everyone trusts the technician without a doubt.

Social engineering is also present in the offline world. Police officers, journalists, and sellers use interesting techniques. For example, the police use social engineering when the law interferes with obtaining data "We do not blame you for anything, just tell us how it was" - the simplest example of circumventing article 63 of the Constitution of Ukraine "A person is not responsible for refusing to testify or explain against family members or relatives." Another example: the gangster

dilemma is a fundamental problem in game theory, according to which players will not always cooperate with each other, even if it is in their interests [3].

Another social engineering application is re-pronouncing product information, links to authoritative or expert opinion, the use of stereotypical images, they all are the most popular tricks used by advertisers. Media - they also resort to social engineering - imposition of thoughts, false cause-and-effect relations, manipulation of feelings, substitution of concepts can occur.

The sphere of social engineering is limitless, but in order to withstand psychological pressure easily, you need to follow some simple rules: when entering into any type of communication, pay attention not only to the content, but also to the process, ask yourself the question "What can all it mean?" more often. Psychologically, games are different, but their essence remains unchanged, a critical attitude to the incoming information, vigilance and common sense will help not to become a victim of a social engineer.

REFERENCES

1. Social engineering [Electronic resourse].-Electronic data. Mode of access: https://en.wikipedia.org/wiki/Social_engineering_(security) – Title of the screen
2. Phishing is a cybercrime [Electronic resourse].-Electronic data. Mode of access: http://www.phishing.org/what-is-phishing – Title of the screen
3. What is Social Engineering on Social Media? [Electronic resourse].-Electronic data. Mode of access: https://www.digitalndigital.com/social-engineering-on-social-media/ – Title of the screen