Implementation of Social Engineering Attack at Institution of Higher Education

Zhengbing Hu [1] [0000-0002-6140-3351], Volodymyr Buriachok [2] [0000-0002-4055-1494], and Volodymyr Sokolov [2] [0000-0002-9349-7946]

[1] Central China Normal University, Wuhan, China
hzb@mail.ccnu.edu.cn
[2] Borys Grinchenko Kyiv University, Kyiv, Ukraine
{v.buriachok,v.sokolov}@kubg.edu.ua

Abstract. The paper shows an investigation utilizing assaults, for example, a phony passage and a phishing page. The past distributions on social building have been checked on, insights of separations are investigated and bearings and component of acknowledgment of assaults having components of social designing are examined. The information from the examination in three better places were gathered and investigated and the substance measurements were given. For examination, three classifications of advanced education organizations were picked: specialized, helpful and blended profiles. Since the exploration was led in instructive organizations during the week, most understudies in the test and graduate understudies partook in the test. For each instructive establishment, an enrollment structure layout was made that emulated the plan of the principle pages. Instances of equipment and programming execution of an average represent assault, information accumulation and investigation are given. So as to develop a test stand, generally accessible segments were picked to show that it is so natural to complete assaults of this sort without critical introductory expenses and uncommon aptitudes. The paper gives measurements on the quantity of associations, consent to utilize the location of the email and secret word, just as authorization to consequently move administration information to the program (cookies). The insights are prepared utilizing uniquely composed calculations. The proposed ways to deal with taking care of the issue of socio-specialized assaults can be utilized and executed for activity on any objects of data action.

Keywords: attack, fishing, social engineering, wireless access point, protection, personal information.

1 Introduction

Nowadays, all businesses are involved in the processes of storing and processing information. This information may contain sensitive information, the disclosure of which will cause significant damage to the reputation of the company, its working capacity or financial position.

 CybHyg-2019: International Workshop on Cyber Hygiene, Kyiv, Ukraine, November 30, 2019.

Social engineering is not about computer technology, it's about the user. Of interest are all solvent persons, as well as users with valuable information, employees of enterprises and public institutions. This method is used for financial transactions, hacking, data theft, such as client databases, personal data, and other unauthorized access to information. Social engineering helps competitors to scout, identify weaknesses in an organization, entice employees.

2 Review of the Literature

The issue of social engineering in domestic academia has emerged at a time of dramatic increase in the availability of information resources, telecommunications networks and user terminals. Principles of influence on a person through social engineering are given in [1]. General issues of data leakage are discussed in [2] and [3], and directly social engineering—in [4] and [5]. The problem of providing access to business information is discussed in [6] and [7].

3 Problem Statement

Worldwide Information System Crash Statistics as of 2018, according to Verizon Communications Inc. is presented in Fig. 1 [8]. According to these statistics, social engineering ranks third in the number of attacks.

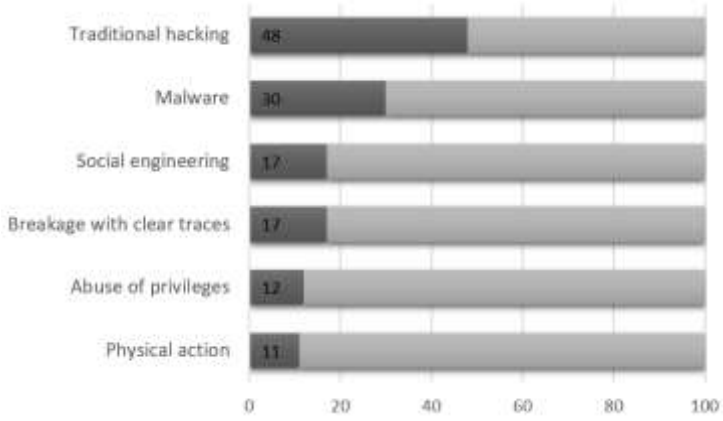

Fig. 1. Cracking tactics statistics

There are many sources of threats to enterprise information and cyber security. The staff of the enterprise is always involved in the process of storing and processing information. Therefore, it is important to consider the anthropogenic factor as a real existing vulnerability in the information security of the enterprise. According to statistics, social engineering is the most significant threat to the anthropogenic factor.

There are many methods of counteracting social engineering. One such method is to raise staff awareness of counteracting social engineering methods. Not all businesses pay due attention to awareness. Therefore, it becomes necessary to create an effective methodology for raising staff awareness of counteracting social engineering methods.

The purpose of the work is to prepare a sound methodology for raising the level of awareness of staff in countering social engineering methods. The object of the study is the process of managing staff awareness. The object of the study is to counteract social engineering methods.

The scientific novelty of the work is to develop a methodology for managing personnel awareness in countering methods of social engineering. The practical value lies in developing methodological guidance to raise staff awareness of counteracting social engineering methods, as well as developing a questionnaire to analyze the level of awareness.

All the work done is done solely within the scope of the study to determine the level of user awareness. All sensitive user information, such as passwords, is not disclosed or stored in the public domain to protect them. The organizer of the research reserves the right to store, process and publish all collected data, in accordance with the terms of use of the service, each user who sent the data previously agreed to the terms of use of the service.

4 Theoretical Basis

In the context of information technology, social engineering is a set of applied social science approaches that focus on the purposeful change of organizational structures that define and control human behavior, or a comprehensive approach to the study and change of social reality based on the use of engineering and technology approaches.

Social engineering is used for:

– gathering information about the purpose of the enterprise;
– receiving confidential information;
– direct access to the system.

In information security, the term “social engineering” is used to describe the science and art of psychological manipulation. According to Infowatch’s think tank, 55% of losses related to information security breaches stem from the fault of employees who have come under the influence of social engineers [9].

In educational practice, the ideas of social engineering are realized through the use of modern educational technologies and active teaching methods, as well as through the “saturation” of the educational process by the disciplines of the sociological and organizational cycle, including:

– theory and methods of social engineering;
– diagnostics of organizations;
– forecasting and modeling of development of organizations;
– organizational design and programming;
– social planning;

– introduction of social innovations in the organization;
– social technology workshop;
– methods of conflict resolution.

Basically, social engineering incidents related to staff actions occur because of low levels of user awareness. Thus, by educating their staff on the basic rules in information security, organizations can significantly reduce the risk of information security breaches. No wonder, staff training is one of the main requirements of the international standard for information security management ISO/IEC 27001 [10].

Features of attacks using the human factor:
– do not require significant costs;
– do not require special knowledge;
– can last for a long period;
– difficult to track.

A person is often much more vulnerable than the system. This is why social engineering is aimed at obtaining information through a person, especially in cases where it is impossible to access the system (for example, a computer with important data is disconnected from the network).

There are several techniques in social engineering that are used to accomplish these tasks. All of them are based on the mistakes made by a person in behavior [11].

Social engineering techniques include:

1. Phishing attacks are the most popular type of fraud in social engineering. Phishing attack is the illegal acquisition of sensitive user data (login and password). Often, phishing emails are written poorly and contain grammatical errors. In these letters, the attackers point to a hyperlink to a copy of the site (for example, a mail client) with a form where you need to enter your login, password and other personal information. For example, phishing is used to collect user logins and passwords by sending letters and messages prompting the victim to provide the necessary information. You can protect yourself from abusers by ignoring letters from unknown recipients.

2. Pretexting is an attack conducted in advance prepared scenario. Such attacks are aimed at developing a victim's sense of trust in the attacker. Attacks are usually made over the phone. This method often does not require the preparation and retrieval of victim data. Pretexting is about extraditing oneself to another person to obtain the desired data. You can get information about a person through open access sources, mainly from social networking pages.

3. The Trojan horse uses the qualities of a potential victim, such as curiosity and greed. A social engineer sends an email with a free video or an antivirus update in an attachment. The victim saves the attachments, which are actually Trojan programs. This technique will remain effective as long as users continue to mindlessly store or open any attachments.

4. Quid pro quo. When using this type of attack, the attackers promise the victim a benefit in return for the facts. For example, an attacker calls the company, introduces a support staff, and is offered to install the "necessary" software. Once the consent to the installation of the programs has been obtained, the offender shall have access to the system and to all data stored in it.

5. Feedback implies an unauthorized passage of an attacker along with a legitimate user through a checkpoint. This method should not be used in companies where employees need to use passes to enter the territory of the company.

6. Shoulder surfing is one of the social engineering techniques. It is used in transportation, cafes and other public places that allow the victim to monitor computer devices and phones through the victim's shoulder. There are situations in which the user himself offers the fraudster the necessary information, being confident in the decency of the person. In this case, they are talking about reverse social engineering.

7. Threats when using instant messaging. Users quickly appreciated the convenience of messaging in real time using the Skype, Viber, WhatsApp, Telegam, and other networks. The accessibility and speed of this method of communication makes it open to all kinds of attacks. For security, you should ignore messages from unknown users, do not give them personal information, do not follow the links sent.

It is obvious that social engineering can do enormous damage to any organization. That is why every effort should be made to prevent human factor attacks [12,13].

Initially, the purpose of influencing a particular object is always formed. "Object" refers to a victim targeted by an attacker.

Then, information about the object is collected to identify the most suitable targets of impact.

Then comes the stage that psychologists call attraction. Attraction is the creation of the necessary conditions for the attacker to influence the object.

Forcing a social hacker to take action is usually achieved by performing the previous steps, that is, once the attraction is reached, the victim creates the actions that the attacker needs. However, in some cases this stage becomes independent, for example, when the compulsion to act is accomplished by introducing into a trance, psychological pressure, etc.

All attacks by social hackers fit into one fairly simple scheme (Fig. 2).

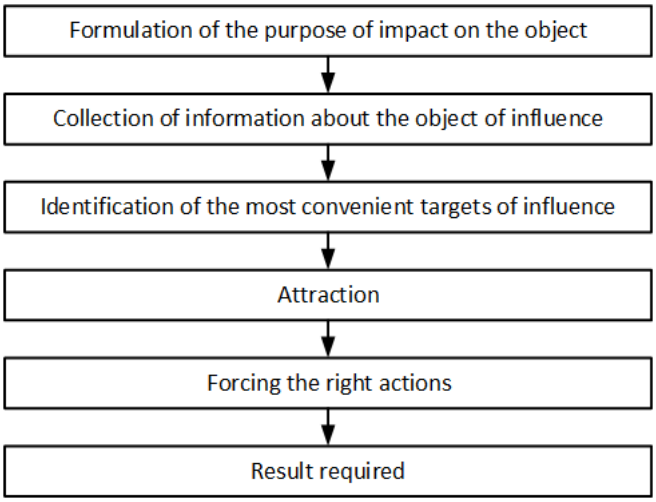

Fig. 2. The main scheme of influence in social engineering

5 Method of Research

Usually, for the convenience of people, most public Wi-Fi networks are left open, making them a good place for a variety of attacks. This fact is the inspiration for this study.

So it was decided to create an open Wi-Fi network to collect data from the victims as follows:

– ability to connect to a wireless network for anyone;

– pseudo-interface for registering a user on a network whose primary task will be to collect the victim's data, including the data it will provide us and the data we receive from the victim's browser, namely the User-Agent and Cookies for the domain that the victim wanted to access. us to use its authentication on this domain;

– adjust the equipment so that it can operate in full offline mode;

– put the equipment in places of crowds of people;

– pick up the equipment in a week (high capacity batteries should be used to achieve autonomy).

The following hardware is included in the experiment:

– miniature single-board, energy-efficient computer based on ARM architecture with the ability to connect devices via USB;

– USB-MicroUSB power cable;

– portable battery (power bank) with USB interface;

– 802.11n wireless network adapter with USB interface and external antenna;

– USB-USB extender for easy placement of elements;

– MicroSDHC Class 10 memory card.

The following equipment was selected for the test bench: Raspberry Pi 3 Model B, SanDisk MicroSDHC 16Gb Class 10, Trust PowerBank 10 000 mAh, Tp-Link TL-WN722N v3. In Fig. 3 shows a test bench in its assembled and on state.

Fig. 3. The appearance of the test bench

To implement the fake hotspot and phishing interface, the following software toolkit has been defined on it:

– *hostapd* is Wi-Fi hotspot service;
– *dnsmasq* is DHCP and DNS server;
– *lighttpd* is web server;
– PHP is web server programming language;
– HTML is CSS and JavaScript stack for browser representation;
– *SQLite* is database for storing data.

As part of the experiment, three profiles of higher education institutions were selected:

– technical (State University of Telecommunications, Kyiv);
– humanities (Borys Grinchenko Kyiv University, Kyiv);
– mixed (Lviv Polytechnic National University, Lviv).

A separate phishing website was developed for each of them (Fig. 4 shows an example of a page for (Borys Grinchenko Kyiv University).

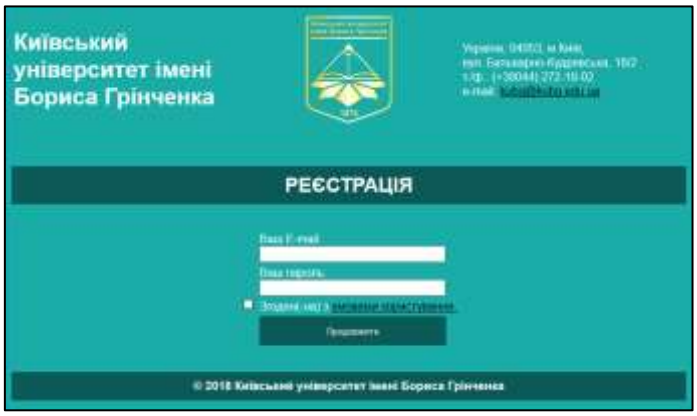

Fig. 4. An example of a fake web page for Borys Grinchenko Kyiv University.

The terms of service (privacy policy) have been developed for the validity of this study. Agreeing to the privacy policy of the user before sending the data gives the organizer a legitimate reason for storing, processing and publishing this data. The access point did not have internet access, so the data was collected only the first time, the data was stored only as statistics.

6 Research Results

While analyzing the results, there was a need to automate the information processing and data linking process. In particular, the following program was written in C#/.NET v. 4.5 to create mappings between MAC and IP addresses and actions on the web server.

The study provided technical data (operating system, browser version, mobile device manufacturer, etc.), behavior data (reconnection) and user data (email, passwords, cookies, request to the target site). Of all the data, the most valuable value for social engineering research is the behavior and personal data that users have agreed to share.

A good indicator of internet accessibility is the percentage of reconnections. From the diagram in Fig. 5 shows that the number of attempts to reconnect does not depend on the profile of the institution of higher education, but only on the availability of alternative wireless networks.

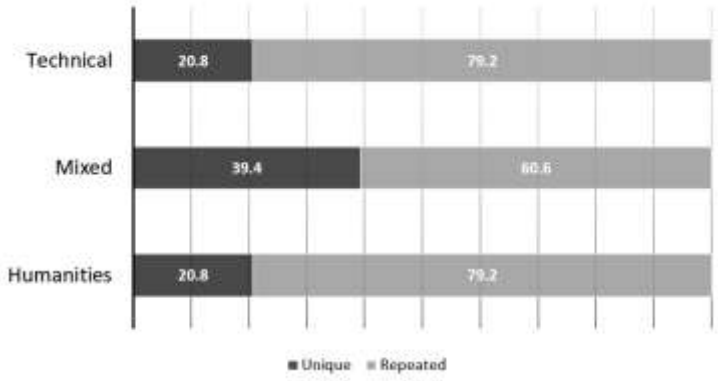

Fig. 5. Connection statistics

The statistics on the ease with which users share their email address and even their passwords are shown in Fig. 6. The trend shows an increase in the percentage of personal data provided by students in the humanities profile, but still the trust in unknown open networks is quite high among the students of technical higher education institutions. The high percentage of password entry is due to the input of non-existent passwords.

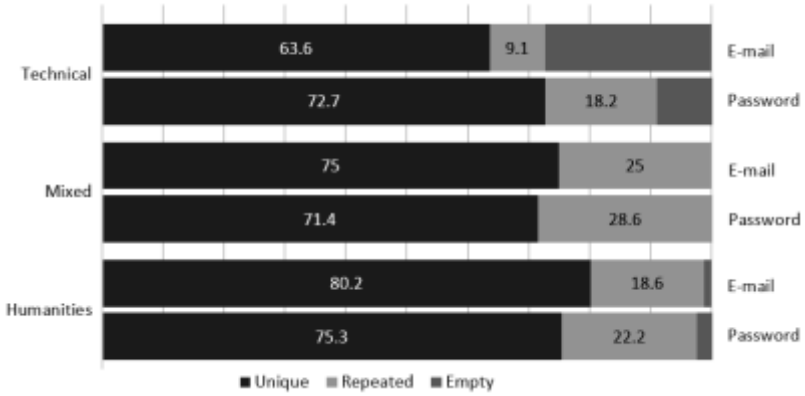

Fig. 6. Insertion of personal data (email and password)

The issue is the openness of cookies, because to get more functionality from web resources, most users allow this data to be exchanged without a single request for data transfer. From Fig. 7 shows that the number of users sharing a cookie depends only partially on the profile of the institution of higher education. Therefore, the issue of cookie openness should be considered as a general danger of data exchange, and not just as an aspect of social engineering.

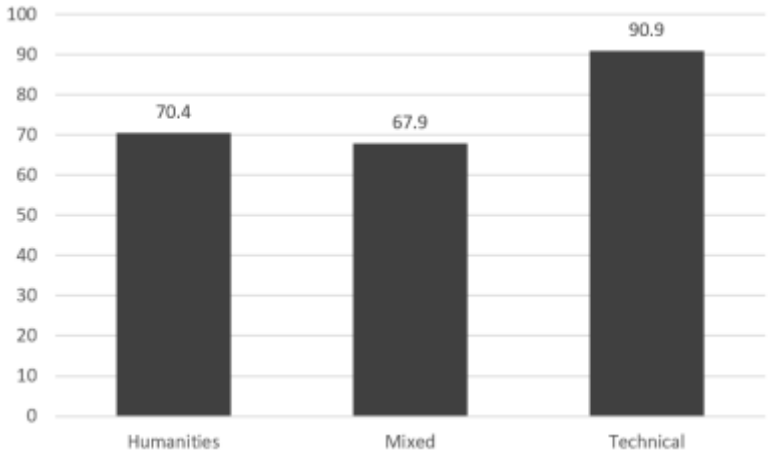

Fig. 7. Cookie permissions statistics

7 Acknowledgments

This scientific work was partially supported by RAMECS and self-determined research funds of CCNU from the colleges' primary research and operation of MOE (CCNU19TS022).

8 Conclusions and Further Research

During the work there were problems in the configuration of the *lighttpd* software. By default, this web server does not use logging of all hits, unlike Apache *httpd*. Therefore, statistics such as device manufacturers from devices that provided Web server data are not available at the State Telecommunication University. This fact was taken into account and the number of information collection points was increased to three.

During the work, a number of problems were solved related to logging, automation of data analysis and processing, configuring IPv4 network addressing, intercepting all user requests, and more. Issues resolved regarding reconciliation between data collected by different software.

The main task of the work is to investigate the awareness of users regarding social attacks, it was solved and sufficient statistics were obtained during the study. Because the test bench is built on widely available components and open source software, this kind of attack can easily be replicated by anyone with a technical background in computer engineering and information security.

Experiments show that users' awareness of even the technical specialties is insufficient, so special attention should be paid to developing techniques for raising user awareness and reducing the number of potential attacks on information objects.

References

1. Nemtseva, O. O.: The notion of informational and psychological influence. Soc. Commun.: Theory Pract. **1**: 55–66 (2015) [Ukrainian].
2. Emelyanov, S. L., Nosov, V. V.: Ways and channels of information leakage from a typical object of informatization. Law Saf. **1**: 273–279 (2009) [Ukrainian].
3. Filippova, L. Y.: Information paradigm of social communication (review of scientific approaches and concepts). Bull. Kharkiv State Acad. Cult. **39**: 79–86 (2013) [Ukrainian].
4. Dashko, D. A., Meshkov, V. I.: Social engineering from the point of view of information security. In: V Ukrainian Conference "ITBtaZ," pp. 1–2. DVNZ "NGU," LLC "Salvia," Kyiv (2013) [Russian].
5. Daddyuk, A. V., Petryk, V. M.: Counteraction to Automated Means of Using Social Engineering. In: IX All-Ukrainian Scientific and Practical Conference "Actual Problems of Information Security Management of the State," pp. 346–347. NASBU, Kyiv (2018). [Ukrainian].
6. Navrotsky, Y. Y., Patsey, N. V.: Implementation of caching policies in information-oriented networks. In: Proceedings of BSTU, vol. 3(1), pp. 99–103, Minsk (2018) [Russian].
7. Fan, W., Lwakatare, K., Rong, R.: Social engineering: I-E based model of human weakness for attack and defense investigations. Int. J. Comput. Netw. Inf. Secur. **9**(1), 1–11 (2017). DOI: 10.5815/ijcnis.2017.01.01
8. Verizon Communications: Data breach investigations report. 11th edn., 68 p. (2018).
9. InfoWatch: Modern threats emanating from information systems. 12 p. (2017) [Russian].
10. International ISO/IEC standard 27001:2013. Information technology. Methods of protection. Information security management systems. Requirements. 34 p. (2013) [Russian].
11. Shatkovsky, M. O.: The influence of social engineering on the information security of organizations. NTUU "KPI", Kyiv (2015) [Ukrainian].
12. Anisimova O., Vasylenko V., Fedushko S. Social Networks as a Tool for a Higher Education Institution Image Creation. CEUR Workshop Proceedings. – 2019. Vol 2392: COAPSN-2019. P. 54–65. http://ceur-ws.org/Vol-2392/paper5.pdf
13. Sokolov, V. Y., Korzhenko, O. Y.: Analysis of recent attacks based on social engineering techniques. In All-Ukrainian Scientific and Practical Conference of Higher Education Applicants and Young Scientists "Computer Engineering and Cyber Security: Achievements and Innovations," pp. 361–363. CNTU, Kropyvnytskyi (2018). DOI: 10.5281/zenodo.2575459.