Memoirs of the Scientific Sections of the Romanian Academy
Tome XL, 2017

COMPUTER SCIENCE

CONSIDERATIONS ON PREVENTING SOCIAL ENGINEERING OVER THE INTERNET

MIRONELA PÎRNĂU

"Titu Maiorescu" University, Faculty of Informatics, Bucharest, Romania
Corresponding author: mironela.pirnau@utm.ro

The decrease of personal interactions, caused by the development of modern communication instruments (e-mail, Facebook, Twitter, Skype, Dropbox, LinkedIn, Lync etc.) has allowed the evolution of new methods of social engineering attacks, which, under certain conditions, may become a very dangerous weapon.

The aim of the present paper is to offer an overall presentation of possible attacks based on social engineering. The paper aims at identifying the specific methods of social engineering, as well as at displaying the defensive techniques in case of social engineering attacks. In the present-day society, based on Internet communication, it has been observed that the art of social engineering represents a phenomenon which continues to grow, because of the low costs of the attacks.

Keywords: social network, social engineering, attack.

INTRODUCTION

Social engineering has evolved, being identified by many terms, and various shapes, including defrauding and cheating methods and techniques, targeting different purposes and benefits. According to the Greek mythology, even since Antiquity, one of the forms of social engineering was that of the Trojan horse. There are also many other examples [8, 14, 22] of people manipulated through social engineering methods, and forced to act in a manner in which they would not act if they analyzed the respective actions better. The present paper contains five sections, which include: (1) introduction, (2) main social engineering methods, (3) techniques used to conduct a social engineering attack, (4) case study and (5) conclusions. The present paper underlines only a small part of the ways in which the user case be exposed to social media attacks, when new technology is used.

SOCIAL ENGINEERING METHODS

Literature studies [1, 4, 8, 18, 21] have shown that hackers may obtain important information through simple methods, accessible to anyone who possesses persuasion, defrauding and cheating capacities used on the Internet. The applied techniques of social engineering are extremely efficient, and can be applied to numerous users (especially to those who can be easily influenced).

Kevin Mitnick [23, 24], a consultant in information security, states that a company may spend hundreds of thousands of dollars investing in firewalls, in systems detecting intrusions, in security encryption systems [33] and in other security technologies, however, if an assaulter appeals to a trustworthy person within the company, and if the respective person agrees to cooperate, and the assaulter receives the access, then all investments in the above-mentioned technologies have been wasted. The information technology interacts and affects all components of human existence: human mental condition, industry, economy, security, and political world [14, 17, 20].

THE PSYCHOLOGICAL MANIPULATION OF PEOPLE

Among the main human weak features that contribute to the success of the social engineering techniques, mention should be made of: greed, fear, the feeling of urgency, curiosity, sympathy, the respect towards authorities or trust in a certain person, etc. [11, 14, 23, 26].

Greed – the most common form of social engineering is represented by messages through which the assaulter tries to benefit from the greedy targeted victim. "Hey, I have a great sum of money and I promise to give you half of it if you offer me some information about yourself".

Fear – the assaulter may frighten the victim so that the latter should act differently than in the usual manner. In this case, the assaulter relies upon victim's fear, blackmails him/her, claiming that he/she has sensitive information about the victim and, if the victim does not pay a requested sum of money, the information will be made public over the Internet.

The feeling of urgency – the assaulter (usually by means of marketing campaigns) persuades the victim over a profitable offer.

Curiosity – is revealed as various articles, images and films containing words and phrases such as: "*shocking*","*you won't believe it*", "*sensational*", and so on, with the intention of making people become curious and click on the message. Thus, curiosity challenges people to react differently than they would normally do (Fig. 1).

Fig. 1. Curiosity.

Sympathy – using fraud methods, the assaulters tell stories about most unpleasant topics, with sensitive content, in order to gain the *sympathy* of the victim: "We were attacked in the hotel we were lodged", and sums of money are requested, money the criminals promise to return – which never happens.

Respect towards authorities – the victims think that they communicate with the manager of the company they work for, with their superior or with one of the officials. However, if the targeted victim had clicked on any of the links, the computers would have been infected with a ransomware.

Trust in a certain person – the victims receive messages that seem to be delivered by trustworthy people, teachers, mentors, etc. Actually, the links included in these messages may be malicious and dangerous. The links must be carefully analyzed before being accessed, even if they seem to be sent by reliable people [7, 16, 32, 38].

The scheme presented in Figure 2 proposes an analysis method of an email.

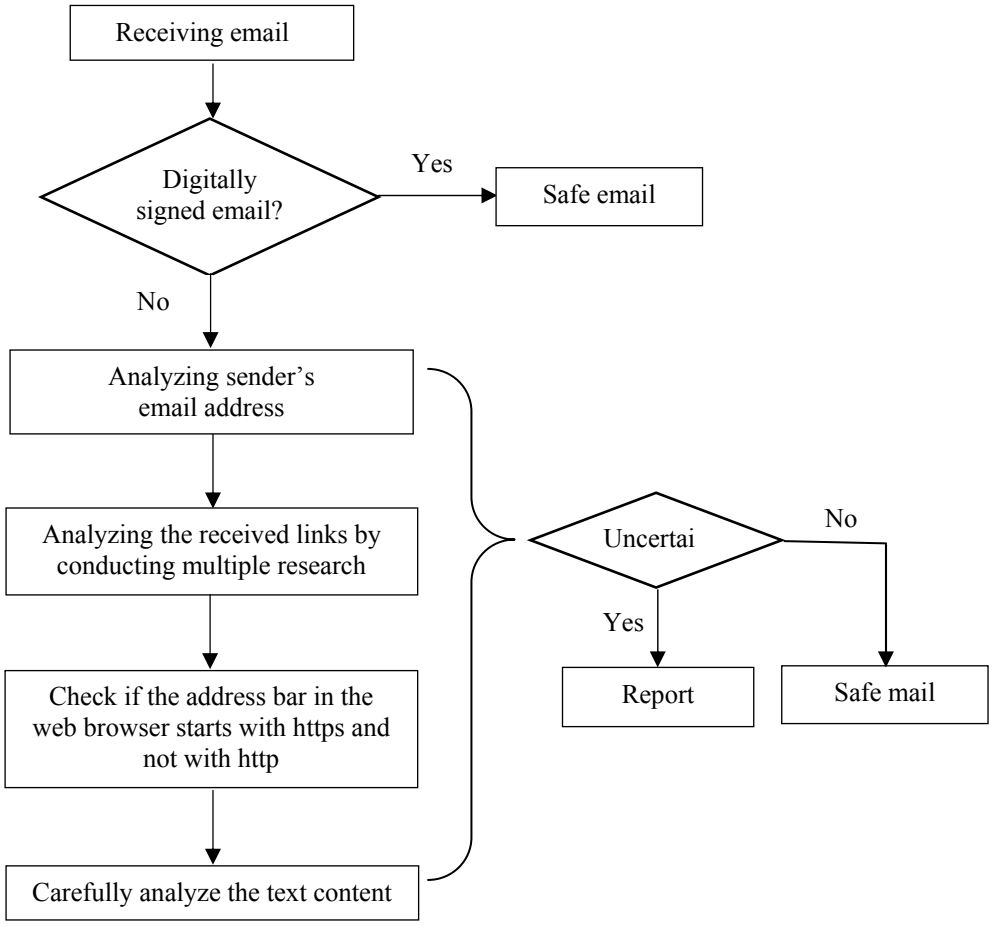

Fig. 2. Scheme for checking a link.

THE PHISHING ATTACKS

The phishing attacks occur when they are attempted at determining potential victims to send personal information online. The phishing websites may request sensitive information, such as: usernames, passwords, personal identification number, credit card details, PIN codes, maiden names, birth dates, etc. The phishing attempts represent the most efficient mechanism of social engineering [7, 15, 18]. Cybernetic criminals use social engineering methods to determine users to access compromised websites, aiming at tricking people into installing malicious software, or into disclosing personal or corporate information. In order to analyze an email for identifying a possible phishing attack, the following aspects should be taken into account:

– Spelling and grammar mistakes – if these types of errors are to be found, it is most likely that users are the target of a scam.

– The links *via* an e-mail – the existence of a link in the text body of an email must be carefully examined. It is advisable to place the mouse on the link and check if the respective address matches the link. The links may lead to infected websites or folders.

– Cybercrime threatening – Cybernetic criminals usually threaten users that the email account security will become vulnerable.

– Spoofing sites – several graphics are used in the body of the email graphics, that seem connected to legitimate websites, but in fact they sled the readers to hoax sites or to pop-ups that seem legitimate. Cybernetic criminals also use slightly modified web addresses that resemble famous well-known brand names or companies [2, 6, 28].

A May 2017 statistics (http://www.phishtank.com/stats/2017/05/), reported by PhishTank free community site (which offers an opened API for researchers and developers to integrate anti-phishing data in their applications free of charge) show that the majority of phishing attempts have been aleatory. As a defending measure against this type of attack, the browsers include the possibility of reporting a suspected scam on the web or in an email. Google is concerned with this situation and, in order to report them, it provides an online form to be filled in.

PEOPLE AS VULNERABILITY AND RISK

Many of the social engineering attacks are successful because people are vulnerable, and they can be easily manipulated in various ways. The social networks providers rely on a business pattern based on a type of publicity focused on certain public sectors. These companies have hundreds of thousands of users for their services and thus, a vital interest in collecting as much information as possible [23, 35]. The regular leaks of collected data from users by using security breaches represent a real threat for confidential data.

In the context of online social networking, Gross and his collaborators [13] identified several threats to privacy, such as tracking and making medical records public.

At present, Facebook is the social network with the largest number of active users and it has been critical for personal data leaks and preferences for third parties sites, tricking the users into accidentally sharing private data, because of privacy settings, by tracking users' browsing behavior, whether they were disconnected or not, without consent, disregarding the privacy rules [9]. The main behavior features include (but do not refer only to) [5, 10, 27]:

– *The joy of victory* – the attacker sends an email which stirs a state of joy, then influences the victim to download a malware program in the car software, in order to provide victim's distance access to the car.

– *Fear of Authority* – as there are so many people who let themselves intimidated by authorities, attackers use their psychological weakness to obtain the targeted data.

– *The desire to be helpful* – based on the wish of becoming helpful, the attackers succeeding in discovering a great number of data, which normally would not be revealed to a stranger. All this data allows the attacker to get unauthorized access to the targeted system.

– *Fear of Loss* – the criminal sends an email to the victim, informing that a serious sum of money was won but just a small amount of it must be deposited in a certain bank account. Out of fear of losing such an opportunity, the victim makes a deposit in the provided bank account, and then realizes that it was a scam.

– *Insufficient knowledge* – this type of attack is based on an insufficient training of the employees. Social engineers take advantage of this weakness, creating the feeling of urgency, so that the employee does not have sufficient time to correctly analyze the situation, thus becoming the victim of an attack.

TECHNIQUES USED TO CONDUCT A SOCIAL ENGINEERING ATTACK

By imitating some trustworthy sources and by exploiting the human psychology. Social engineering succeeds in obtaining personal data. By making these types of common social engineering attacks public, many other cases may be prevented or diminished [3, 12, 25, 28]. The most common techniques in conducting a successful attack [37, 38] are:

Shoulder surfing – a type of attack in which the attacker uses observation techniques such as searching over someone's shoulder, in order to obtain data, while certain actions – that involve the explicit use of sensitive visible data – are performed.

Role playing – involves the use of an online chat session, of an email, of a phone call or of other methods by which the company uses to interact with its public online.

Trojan Horses – the most frequent method by means of which victims are determined to download a malware file. This file is actually a backdoor which will be used by the assaulter to obtain complete access to victim's computer.

Watering hole attacks – they are more subtle than phishing attacks, being based on the incorporation of a malware into a trustworthy site, which is already targeted by the assaulter. This process starts with a technical exploit in the code of the web, but it is successful only if the victim clicks on the malicious link.

Pretexting – the attackers define a false scenario in order to manipulate the victims into revealing data, a common technique to involve the attackers who demand for information in order to confirm victim's identity.

Tailgating – this attack depends on how quickly people's trust is gained, for obtaining access to physical locations. In order to be protected against this type of attack, it is advisable to be cautious with the identity of all strangers who have access to a secure location, even if they prove their identity.

Baiting – by using these types of attacks, the potential victims are offered free music downloads, software programs, which obviously contain malware programs. This method is common when using illegal torrent or other types of downloads that do not take account intellectual property or copyright laws.

Dumpster Diving represents a frequent method of social engineering based on techniques of looking into the recycle bin, searching for potential useful data placed there by the employees of a certain company.

Reverse Social Engineering – the hacker sabotages a certain network, thus causing a problem, then he promotes himself as being the right person to solve the problem. The employees never know that there was a hacker because the problem was solved, and everybody was happy.

CASE STUDY

Based on numerous theoretical and practical studies [19, 25, 27, 29, 30, 34] as well as on the experience gained in the field, this case study draws attention to certain possible types of vulnerabilities related with social engineering. The aim of these personal interpretations is to reveal the multitude of present cases in which someone might become a victim of social engineering [31].

YAHOO MESSENGER VERSION 0.8.288

It is a well-known fact that, for becoming safer, Yahoo has continuously improved its versions. Taking into account the former Yahoo Messenger, only one

vulnerability will be mentioned here – which might be explored nowadays, if the attacker uses the Dumpster Diving method, and if we are not sufficiently cautious (see Section 3) [23, 30]. The vulnerability consists in the fact that, after logging out from Yahoo-Messenger, the ID of the people the victim chatted with still remains on the related station. To avoid this, if there are still old systems used to log to the Yahoo Messenger account, the XML file from the following path is to be found: *C:\Users\admin\AppData\Local\VirtualStore\Program Files (x86)\Yahoo!\Messenger \ Profiles* agenda. In the path:
C:\Users\admin\AppData\Roaming\Yahoo!\Messenger\id-ul user, there is a certain folder for each "member" in victim's personal agenda. As one may notice, in the here presented case, these paths contain an admin as work user, and, in order to be visible, all these folders should have the visibility option active. Even if Yahoo dealt with this vulnerability and solved the problem, there still remains the risk that, by using the Dumpster Diving method, the users become potential victims of a social engineering attack, if the old supported systems were not cleaned.

Starting with June 2013, Yahoo closed the Yahoo Mail Classic interface and users are forced to use a new interface, improved in terms of visibility and security. For improved safety, Yahoo provided its users a new version of Yahoo Messenger on 31st August 2016, when the old versions became unavailable. In case one user wants to have access to the previous conversation archive in the old Yahoo Messenger version, then old conversations can be found by using the following link: https:// messenger.yahoo.com/archive/.

These are downloadable, in the form of a html folder, which, by using social engineering methods, may become the source of various scams. Another fraud may occur when Messenger is accessed *via* an email account. After signing out from Messenger, there is still access to it and the possibility of sending messages still remains, as well as access to all people in the agenda.

The most sensible issue is that Yahoo does not warn us if users are still connected to their email account or not. This may lead to a social engineering attack if there are individuals who might use the methods provided by social engineering in the vicinity of the user (see Section 3) [15, 19].

FACEBOOK

Most of the social networks, among other web services, are financed by incomes generated by advertising. This may create a conflict of interests as concerns the provider of services, when users' rights and the rights of publicity agencies are to be considered. The users do not want their personal available to anyone, except the parties they explicitly agreed for, after signing an agreement. Moreover, the users desire that their personal data be used only for the exact purpose they agreed for. From user's point of view, any exception made by the provider of services is to be considered disloyal and unfair.

Social engineering and Facebook archives

Facebook provides for its users the possibility of downloading the content of an archive in the personal system. Nevertheless, anyone who subsequently receives access to the respective computer may read or use all user's messages posted on the Facebook platform.

These are saved in an archive with an implicit extremely suggestive name, such as: Facebook-ID, and it can be easily tracked.

This archive contains an index.htm folder (Fig. 3) which allows the visibility of the content of Facebook archive, when opened.

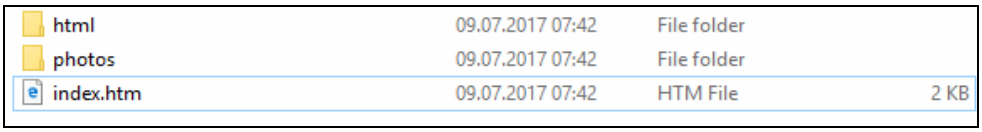

Fig. 3. The content of Facebook_ID archives.

Practically, personal data centralization in one single place may lead to their use by means of social engineering techniques.

ID Facebook log in

One of the methods of getting connected to the Facebook account is to introduce the phone number or a valid Facebook ID. If the phone number is not associated to an ID, then a person's name may be filled in the proper field, and by clicking "recover password", a hacker may "guess" the email address of a user. By revealing the email address of a potential victim (even if it may be public), there is the risk of trying to identify or recover the password (Fig. 4).

Fig. 4. Facebook password recovery.

By the social engineering techniques (Section 3), people may become victims of social engineering if an unauthorized person receives unauthorized access to someone's Facebook account.

Facebook friends list

Many Facebook users block their friends list to preserve their friends' privacy. But not all of these friends have their list of friends blocked. Therefore, a Facebook user, even if his friends' list is blocked, may be tracked by the likes completed, thus becoming a social engineering victim. If, after visiting the profile of a user that has a hidden friend's list, the option View Page Source is accessed, it might be very easy to identify the ***profile_id*** parameter [36]. Because each Facebook id had an identification code attached, and one can see the value associated to the "profile_id" parameter, in the source of the respective page associated to it, such as presented in Listing 1.

Listing 1

:{source:8, ***profile_id:*** *263xxxxxxxxxxxx ,waterfallxapp:"web_react_composer"},uploadEndpoint:"https://upload.facebook.com/ajax/react_composer/attachments/*

After identification of the ***profile_id*** value, photos, likes and photos tagged for the assigned profile become available, even if this has a hidden friends' list, as not all such friends have hidden lists. The list of actions for the above-mentioned viewed element is presented in Listing 2.

Listing 2

https://www.facebook.com/search/263*xxxxxxxxxxxx* /photos-liked https://www.facebook.com/search/ 263*xxxxxxxxxxxx* /photos-tagged

By this method, a person can be tracked by analyzing the photos for which hy received likes, even if his friends' list is hidden. The non-configuration of confidentiality settings of the Facebook profile or their wrong selected setting may create a social profile of the potential victim, based on friends, posts and links to the desired web pages.

LINKEDLN

As many professionals use LinkedIn platform as a business card, they might become vulnerable. Their data could become a starting step of an attack towards a certain company or individual. More than that, in this way a hacker will discover both the security systems used in the network of the company and the specialist

that use them. The LinkedIn profile might also create an overview of all roles and responsibilities the potential victim had or still has within a company, organization, or institution. By using the Wigle.net (https://wigle.net/) website, the attacker might discover the name of the wireless Internet provider of the victim, before getting into contact with the victim, and try the social engineering techniques. The Wingle.net website offers information about the location of different wireless Internet providers on the entire globe. Many LinkedIn users also get in touch with specialists and companies in their field and thus they might receive invitations (links) to be part of online tutorials, by subscribing to them. There exists, however, the danger that the link cannot be trusted, or that the users might be asked to fill in a form with information about the company. The users must be very careful to each piece of information filled in, and above all they should analyze the potential harmful website before sending the data. A helpful method consists in a simple visualization of the source code (Fig. 5) which may reveal a great amount of information about the persons who collect our data, which we provide free of charge, simply by being part of a conference, an online tutorial, a professional meeting, etc.

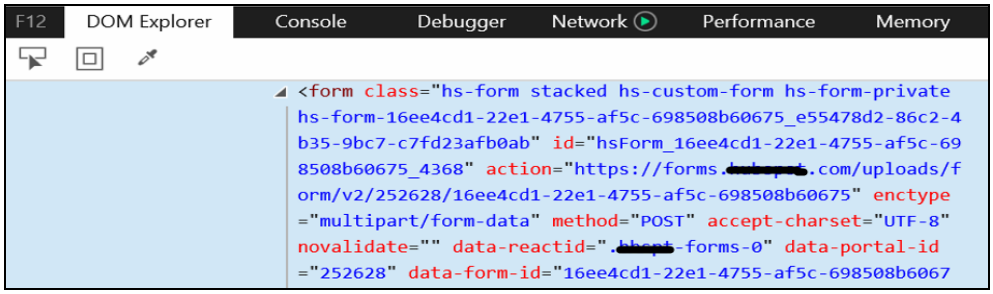

Fig. 5. Code sequence source web page.

CONCLUSIONS

As social engineering is based on the art of influencing and manipulating minds, the online environment is continuously under pressure. When social engineering is based on a digital instrument, the attacker communicates with the victim in a digital manner, without getting in real contact with the victim, most probably by using an email to implement a phishing type of attack, and not only. When social engineering uses methods involving humans, the attacker contacts the victim *via* various methods. Practically, social engineering represents a type of psychological attack where the attacker tries to "influence or determine" the victim to act in the manner which the criminal desires. Actually, this technique represents a type of human manipulation targeting data leakage for subsequent implementation of certain actions based on human weakness, aiming private data theft. In the modern

society, the concern for data protection and information security has been developing continuously, simultaneously with the methods and techniques for data protection. The basis of social engineering is built on various fraud methods and techniques, aiming at different targets and advantages, which may vary from marketing to military actions or cybernetic attacks.

REFERENCES

1. ABRAMOV M.V., AZAROV A.A., *Social Engineering Attack Modeling with The Use of Bayesian Networks*, XIX IEEE International Conference on Soft Computing and Measurements (SCM), 2016, 58–60.
2. ABU-NIMEH S., NAPPA D., WANG X., NAIR S.A., *Comparison of Machine Learning Techniques for Phishing Detection*, Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit. ACM, 2007, 60–69.
3. ANDERSON R.J., *Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition*, John Wiley & Sons Inc., ISBN: 978-0-470-06852-6, 2008.
4. AZAROV A.A., TULUPYEVA T.V., SUVOROVA A.V., TULUPYEV A.L., ABRAMOV M.V., USYPOV R.M., *Social Engineering Attacks: Problem of Analysis, Science*, ISBN 9785-020395923, 2016.
5. BEZUIDENHOUT M., MOUTON F., VENTER H.S., *Social Engineering Attack Detection Model: SEADM*, DOI:10.1109/ISSA.2010.5588500, IEEE Xplore, Conference Information Security for South Africa ISSA, 2010.
6. BLUNDEN B., *Manufactured Consent and Cyberwar*, In LockDown Conference Proceedings, 2010.
7. CHU W., ZHU B.B., XUE F., GUAN X., CAI Z., *Protect Sensitive Sites from Phishing Attacks Using Features Extractable from Inaccessible Phishing Urls*, In Communications (ICC), International Conference on. IEEE, 2013, 1990–1994.
8. CONHEADY S., *Social Engineering in IT Security: Tools, Tactics and Techniques*, McGraw-Hill Osborne Media, 2014.
9. EDWARDS M., BARON A., *Panning for Gold: Automatically Analysing Online Social Engineering Attack Surfaces*, Computers & Security, 2017, (*69)*, 18–34.
10. ELLISON N.B., *Social Network Sites: Definition, History and Scholarship*, Journal of Computer-Mediated Communication, 2007, **13** (1), 210–230.
11. ERKKILA J., *Why We Fall for Phishing*, In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems CHI 2011, Vancouver BC, Canada: ACM, May 7–12, 2011.
12. GIBSON R., *Who's Really in Your Top 8: Network Security in The Age of Social Networking*, In Proceedings of the 35th annual ACM SIGUCCS fall Conference, 2007, 131–134.
13. GROSS R., ACQUISTI A., *Information Revelation and Privacy in Online Social Networks*, In Proceedings of ACM workshop on Privacy in the electronic society, 2005, 71–80.
14. HADNAGY C., WILSON P., *Social Engineering: The art of human hacking*, John Wiley & Sons Inc., ISBN-13: 978-0470639535, 2010.
15. JAGATIC T.N., JOHNSON N.A., JAKOBSSON M.F., *Social Phishing*, Communications of the ACM, 2007, **50** (10), 94–100.
16. JAYAKANTHAN N., RAMANI A.V., *Classification Model to Detect Malicious URL via Behavior Analysis*, International Journal of Computer Applications Technology and Research, 2017, **6** (3), 133–140.
17. JUNGER M., MONTOYA L., OVERINK F.J., *Priming and Warnings Are Not Effective to Prevent Social Engineering Attacks*, Computers in Human Behavior, 2017.

18. KUMARAGURU P., RHEE Y., ACQUISTI A., CRANOR L.F., HONG J., NUNGE E., *Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System*, In proceeding of the IGCHI Conference on Humman Factors in Computing Systems, San Jose, California, USA, April – May 2007.
19. KVEDAR D., NETTIS M., FULTON S.P., *The Use of Formal Social Engineering Techniques to Identify Weaknesses during a Computer Vulnerability Competition*, Journal of Computing Sciences in Colleges, 2010, **26** (2), 80–87.
20. LUO X., BRODY R., SEAZZU A., BURD S., *Social Engineering: The Neglected Human Factor for Information Security Management*, Information Resources Management Journal, 2011, **24** (3), 1–8.
21. MATARACIOGLU T., OZKAN S., *User Awareness Measurement Through Social Engineering*, arXiv preprint arXiv:1108.2149, 2011.
22. MATARACIOGLU T., OZKAN S., HACKNEY R., *Towards a Security Lifecycle Model against Social Engineering Attacks: SLM-SEA*, Proceedings of the Nineteenth Americas Conference on Information Systems, Chicago, Illinois, August 15–17, 2013.
23. MITNICK K.D., SIMON W.L., *The Art of Deception: Controlling the Human Element of Security*, John Wiley & Sons Inc., USA, 2002.
24. MITNICK K.D., SIMON W.L., *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*, John Wiley & Sons Inc., USA, 2005.
25. PELTIER T.R., *Social Engineering: Concepts and Solutions.* Information Systems Security, 2006, **15** (5), 13–21.
26. QI T., *An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering*, In Intelligence and Security Informatics, IEEE, 2007, 152–159.
27. ROSENBLUM D., *What Anyone Can Know: The Privacy Risks of Social Networking Sites, Security & Privacy*, IEEE, 2007, **5** (3), 40–49.
28. RUSCH J., *The Social Engineering of Internet Fraud*, INET Conference, San Jose, CA, 1999.
29. RUTHERFORD A.B.F., *Skinner and Technology's Nation: Technocracy, Social Engineering, and the Good Life In 20th-Century America*, History of Psychology, 2017, **20** (3), 290–312.
30. SCHAAB P., BECKERS K., PAPE S., S*ocial Engineering Defence Mechanisms and Counteracting Training Strategies*, Information and Computer Security, 2017, **25** (2), 206–222.
31. SIADATI H., NGUYEN T., GUPTA P., Jakobsson, M. Memon, N. *Mind your SMSes: Mitigating Social Engineering in Second Factor Authentication*, Computers & Security, 2017, **65** (C), 14–28.
32. SORIO E., BARTOLI A., MEDVET E., *Detection of hidden fraudulent URLs within trusted sites using lexical features*, In Availability, Reliability and Security (ARES), 8th International Conference IEEE, 2013, 242–247.
33. TABUSCA A., *Established Ways to Attack Even the Best Encryption Algorithm*, Journal of Information Systems & Operations Management, 2011, **5** (2.1), 164–168.
34. TEODORESCU H. N., *Revisiting models of vulnerabilities of the networks*. Studies in Informatics and Control, ISSN 1220-1766, 2016, **25** (4), 469–478.
35. TWITCHELL D.P., *Social Engineering in Information Assurance Curricula*, In Proceedings of the 3rd Annual Conference on Information Security Curriculum Development, 2006, 191–193.
36. https://developers.facebook.com/docs/, visiting 01.09.2017.
37. https://usa.kaspersky.com/ resource-center/definitions/social-engineering, visiting 10.09.2017.
38. https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics, visiting 04.08.2017.