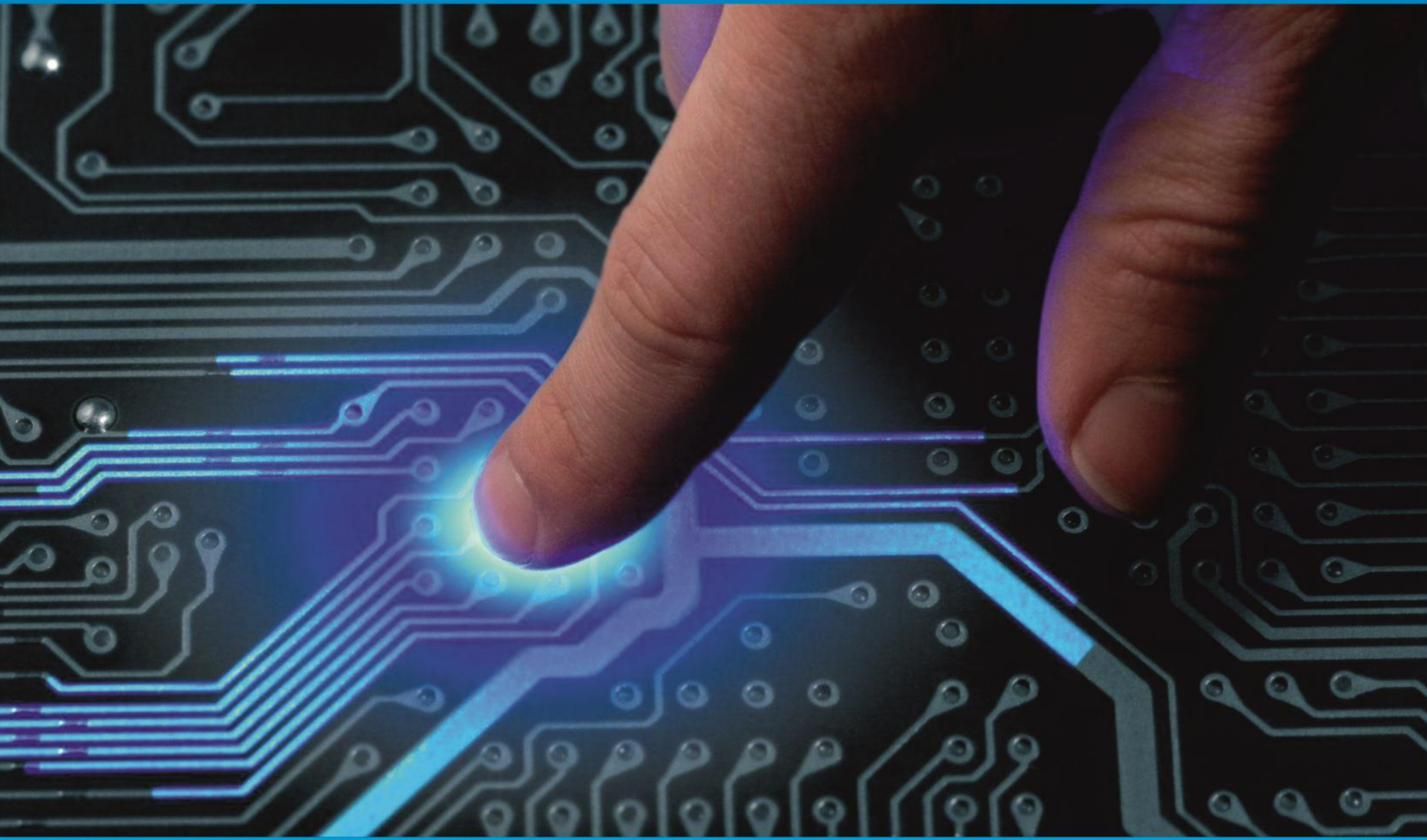
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905039 |

Social Engineering using Malware: Introduction and Psychology

Anjali[1], Nagma Khan[2], Shaily Kushwaha[3], Rajeshwari Gundla[4]

U.G Student, School of Engineering, Ajeenkya D Y Patil University, Pune, Maharashtra, India[1,2,3]

Assistant Professor, School of Engineering, Ajeenkya D Y Patil University, Maharashtra, India [4]

ABSTRACT: Social Engineering (SE) is a technique employed by computer hackers that support people to unknowingly assist the hacker in successfully accomplishing his/her attack. These attacks can be done in two ways. Human-based, where attackers directly make a contact with their targets and get the needed information. Web-based social engineering or Computer-based social engineering attacks manipulate users to perform specific actions, like downloading malware and exposing personal information. We held a survey to test the people for their knowledge of people about social engineering. This paper provides an in depth knowledge of various social engineering attacks, tests whether awareness of social engineering can predict an individuals' security-protective practices, psychology behind susceptibility of people to these attacks and the prevention techniques.

KEYWORDS: Social Engineering, web-based social engineering, computer based social engineering, Malware, security-protective practices, cyber-criminals, psychological dimensions, Awareness programs or methods.

I. INTRODUCTION

As the use of the internet increases, social engineering has become easier to implement compared to the past few decades. While social engineering relies on human behavior, attackers mainly specialize in the psychological instinct of the victims. The success of manipulating employees is generally achieved by establishing a relationship with the victims, trying to build trust. The victims then release some sensitive information as a result of the trust factor. This form of crime is often further classified into piggybacking, tailgating and telephone phishing (vishing). However, within the case of computer-based social engineering, attackers believe computer systems or their technological mode of operation like phishing, fake email, and crop up window attacks. In the last decades, several high-profile cases of social engineering are recorded. Such attacks have resulted in many passwords being leaked. Some of the main victims are global tech giants including Yahoo!, Dropbox, LinkedIn, Facebook, Google, Weebly, MySpace, and lots of others.

When trying to gauge human behavior towards online threats, it's crucial to spot the human factors associated with those threats. According to the prevailing literature, demographic factors, Internet use, and security knowledge are found as a number of the main determinants related to social engineering attacks [2].

The ultimate goal of social engineering psychologically is to form the victim and offer the attacker the knowledge the attacker needs because doing so will benefit the victim. All four attack vectors (that is helpful, carelessness, scarcity and comfort zone) become extremely more complex if the attacker is inside the target organization [3].

WHAT IS SOCIAL ENGINEERING?

The term 'Social Engineering' means deceiving or manipulating a personal to divulge personal or confidential information that may be used for a few malicious purposes [14, 25, 26]. According to Engebretson social engineering is "one of the best methods to collect information about a target through the method of exploiting human weakness that's inherited to each organization" [12].

II. LITERATURE SURVEY

SOCIAL ENGINEERING ATTACKS

Social engineering attacks nowadays are the biggest threats to our data and cybersecurity. [8, 10, 11] The attackers manipulate the users to believe in them and them and exploit them by complying with the commands of the attackers [1]. By complying with the attacker's wishes / commands the users unintentionally create vulnerabilities they enable the attackers to infect their system with malwares and steal the credentials and transfer data [8].

There are 4 stages in which any software engineering attack is done: 1. Reconnaissance/information gathering, 2.Scanning (vulnerability scanning) / elicitation, 3. Exploitation and 4. Post exploitation and maintaining access / leaving without a trace[12, 14, 16, 22].
Let's see these phases in detail.[12, 14, 16, 22]

1. Reconnaissance / information gathering : It is the phase where the attacker finds his/ her intended victim(s) and gathers their background information from social media , search engines, reconnaissance tools , public servers , user sites, blogs ,public reports, etc [16].
2. Scanning (vulnerability scanning) / elicitation: In this phase the victim is engaged by means of appealing to someone's ego, expressing mutual interest, making deliberate false statements, volunteering information, assuming knowledge [16] or by email communication [15].
3. Exploitation: In this phase the attacker executes the attack and steals or takes the required data and can disrupt business or sell the collected data or put it on the dark web[8, 15].
4. Post exploitation and maintaining access / leaving without a trace: in this phase the attackers try to gain more foothold as not everything is permanent and can change or they may have completed the task of gathering whatever they wished for and are now going to remove all traces that there was any malware there or covering all the traces[8].

The social engineering attacks can be classified into two categories i.e. Human based and computer based, based on the entity involved in the attack[8, 23, 25].
Here we will be focusing on computer based social engineering attacks [8, 21, 22, 24].

1. Phishing attack: Phishing is the most popular type of social engineering attack. Phishing scams are like email and text message campaigns aimed toward creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information by clicking on links to malicious websites, or opening attachments that contain malware [8, 21, 22,25].
2. Pharming attack: Pharming combines the words "phishing" and "farming". This cybercrime is additionally referred to as "phishing without a lure". It is a practice through which malicious code is installed on a personal computer or server, misguiding users to fraudulent websites without their knowledge or consent[8,22].
3. Baiting attacks: It uses empty promise to pique a victim's greed or curiosity. In order to cajole users into a trap that steals their personal information or inflicts their systems with malware. Online forms consist of enticing ads that lead to malicious sites or that encourages users to download a malware-infected application [21, 22].
4. Ransomware attacks: Ransomware attacks restrict and block access to the victim's data and files by encrypting them. In order to redeem these files, the victim is threatened to publish them unless paying a ransom[8,22].
5. Scareware: It is a type of malicious software which aims to ensnare users into visiting malware-infected sites and then downloading potentially dangerous applications or purchasing a bogus service. It will appear as legitimate warnings from security services typically in the form of pop-ups or messages from the operating system [8,22].
6. Spear Phishing: Spear-phishing is a targeted plan to steal sensitive information like account credentials or financial information from a particular victim, often for malicious reasons. This is achieved by acquiring personal details on the victim like their friends, hometown, employer, locations they frequent, and what they need recently bought online[22].

7. Reverse engineering: : In this attack the attacker presents himself as a person in a perceived position of authority which influences the victim to ask more questions instead of the attacker. The attacker may seem to solve the problem of the victim but his /her intentions are to gain more knowledge to harm them instead of helping them. The orchestration of such an attack usually spans three stages which are sabotage, advertising and assisting [8,24,26].
8. Pop-up windows: Pop-up window attacks refer to windows appearing on the victim's screen informing the connection is lost or there is a virus on your PC and install the given antivirus. If the user clicks on the install antivirus or reconnects and gives the credentials .He/she installs the malware[8,22].
9. Fake Software Attacks: Fake software attacks also called fake websites. It is based on fake websites which makes victims believe they are known and trusted software or websites. The victim enters real login information into the fake website, which gives the attacker the victim's credentials to use on the legitimate website, such as access to online bank accounts[8,22].

III. PSYCHOLOGY

Humans are the weakest link in security [17]. It is easier to manipulate the human brain. The attackers use compliance as one means by which people can be manipulated. Some of the compliance principles are: - [14, 16, 25, 26]

1. Friendship or liking: If a person who is requesting for compliance is a friend or someone they like, it is more likely the request would be complied.
2. Commitment or consistency: If a person has committed to do something they will comply to request consistent with this position.
3. Scarcity: If there is scarcity or decreasing availability of something people will comply easily.
4. Reciprocity: If a thing has treated them favorably in the past and is being requested in the present it is likely that the request would be complied.
5. Social validation: If people think it is a socially correct thing to do, people will comply easily.
6. Authority: People comply with requests received from people who have more authority than they have.
7. Urgency: Attackers ask you to respond immediately or within 24 hours ,they do not give you much time to think it through so you comply with the urgent request first [4].
8. Emotions: Cybercriminals manipulate the emotions of people and get them to comply with their request[4].

The emotions or expressions targeted in any social engineering attack are:-[4, 16]

1. Greed: the desire to obtain more money, wealth, material possessions or any other entity than one's need.
2. Trust: an abstract mental attitude toward a proposition that someone is dependable.
3. Sympathy/ empathy: they are the emotions experienced in reaction to something that happens to other people or when you quite literally feel the other person's emotions alongside them, as if you had 'caught' the emotions.
4. Revenge: The action of wreaking hurt or harm on someone for an injury or wrong suffered at their hands.
5. Fear: It is a natural, powerful, and primitive human emotion. Fear alerts us to the presence of danger or the threat of harm, that danger can be physical or psychological.
6. Hope: It's a positive state of mind that is supported by an expectation of positive outcomes with reference to events and circumstances in one's life.
7. Sadness: It is feeling down or unhappy in response to grief, discouragement or disappointment.
8. Anger: It is the emotion that you feel when you think that someone has behaved in a discriminatory, brutish, or unacceptable way.

Attackers use reflective responding techniques to gather information from the targets [16]. Here the attacker tries to engage the emotions, feelings and thoughts of the target and try to gain more knowledge and lets the target pour everything out for them to use [20].They try to build instant rapport with their targets by : being genuine about wanting to get to know people, appearing friendly , comfortable and having similar demeanor , being a good listener, being aware of how they affect people, keeping the conversation off of themselves ,being empathetic, being well rounded in general knowledge, finding ways to meet people's need [16].

(*Instant Rapport: making people you meet want to speak to you, want to inform you of their biography , and need to open up to you. Making someone you met recently but feel totally at ease telling him or her very personal things.*)

IV. PREVENTIVE MEASURES

Social engineering attacks are notably troublesome to counter as a result of they are expressly designed to play on natural human characteristics. The human part can continually be vulnerable. Companies are adding multiple layers to their security schemes so that at least one inner layer can help to prevent a threat from turning into a disaster (Risk Mitigation), if all the outer layer mechanism fails. This is known as Defense in depth or multi-layer defense [9]. The following measures can help preempt and prevent social engineering attacks and their combinations are use in Defense in depth: [8, 25]

1. *Security Policy:* A well written policy should include technical and nontechnical approaches that are downward driven by executive management [18,25].
2. *Security awareness training:* Employees must attend initial training during orientation and recurring refresher training in order to get awareness by exposing users to commonly employed tactics and behaviors targeted by a social engineer. Conducting, and continuously refreshing, security awareness among employees is that the first line of defense against social engineering [9, 18,19].
3. *Network Guidance:* The organization has to safeguard the network by whitelisting authorized websites, using Network address translation (NAT), and disabling unused applications and ports. Network users need to maintain complex passwords that are changed every 60 days [8, 25].
4. *Penetration testing:* By using an ethical hacker to conduct penetration testing, you allow an individual with a hacker's skill set to identify and try to exploit weaknesses in your organization. If its penetration succeeds in compromising sensitive systems, it can help you discover employees or systems you need to focus on protecting, or methods of social engineering you may be especially susceptible to[18,19].
5. *Technical Procedures:* The network should have multiple layers of defense to guard data and core infrastructure. Software like Intrusion interference Systems (IPS), Intrusion Detection Systems (IDS) and firewalls ought to be put in on each device. All external facing services must install Demilitarized Zones (DMZ), web filters and Virtual Private Network (VPN) [25].
6. *Antivirus and endpoint security tools:* The basic measure is installing antivirus and other endpoint security measures on user devices [19].
7. *Physical Guidance:* There is a range of options that can be implemented to protect physical assets. In places where physical hardware is located businesses should employ multi factor authentication, biometrics or access control list before access is granted [25].

V. PROPOSED ANALYSIS APPROACH

We held a survey regarding social engineering awareness of people of these attacks that happen.

Firstly people were asked about their age, gender, education and internet usage. On the basis of their age they were divided into 3 categories i.e. age less than 15, 15-36 and above 36.

For children (age less than 15) we checked if they were supervised while user the internet, if they would download any program or files without knowing the place they were supposed to download or not, if they would divulge any personal information to a person whom they do not know or to a virtual friend (related question response in fig. 1 (G)), who had access to all school related data (such as study materials which were shared online , email account of school), do they know about social engineering (response result in fig. 1 (A)), do they think a password of 6-7 characters is strong?

| DOI: 10.15680/IJIRCCE.2021.0905039 |

because strong password criteria plays a vital role in keeping their information secure (survey result in fig. 1 (E)) and if they would install a maybe malware infected program in their phone or PC when they don't have a antivirus present in their PC.

71.4 % children were supervised during their usage of internet, 90.5 % children would not divulge any private information to a stranger while playing games and 95.2 % would not divulge any personal data on social media/ virtual friend, for 52.4% children both them and their parents both had access to any school related data and only 28.6% of the children would install maybe malware infected programs in their PC.

For the people who were 15 above (15-36 and 36 above) they had some scenario based questions and some other questions such as: if the firewall is enabled in their PC or not (response result in fig. 1 (C)), is there any antivirus and if they keep it updated or not(view response result in fig. 1 (B) and (D) respectively), are pop-ups blocked in their browser, if they download form any unknown website, if they click on any unknown links (result shown in fig. 1 (F)) or if they knew the security practices which should be implemented in case of security breach (in fig. 1 (H)).
50% people kept their firewall enabled in their pc , 68.4% people had antivirus installed and 57.9%people kept it updated , 65.8% people blocked pop ups in browser, 75% people ignored the pop ups related to no antivirus.

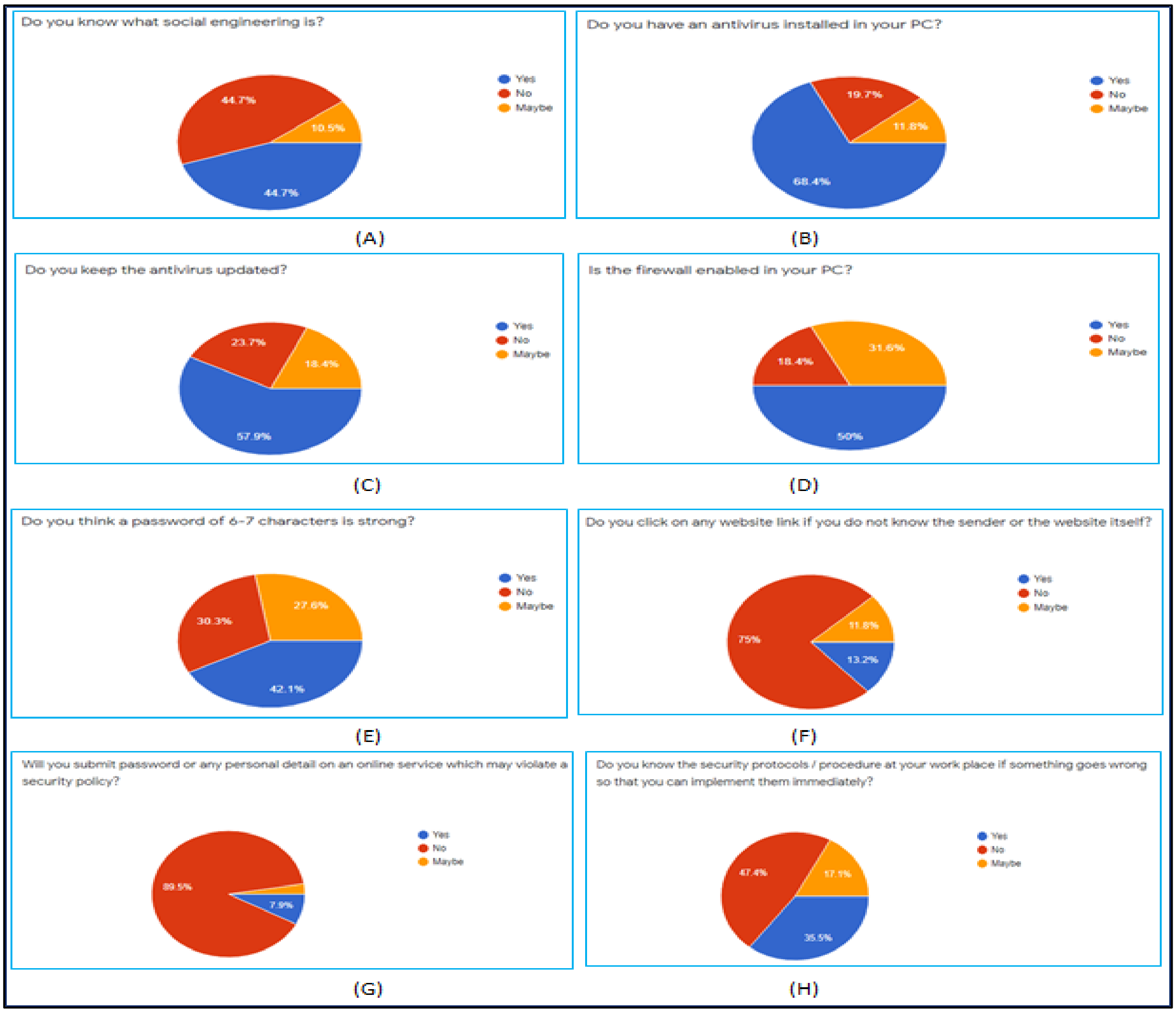


Fig 1: Pictures of Answers from the survey

In all the categories the majority of the people didn’t know what was social engineering or its threats but they still knew some cases where they might get attacked or it could be a scheme to steal their data or belongings. People have taken some or the other preventive measures for it knowingly and unknowingly.

VI. FUTURE SCOPE & DISCUSSION

Future work may analyze these security issues to implement detection and countermeasure techniques to reduce the success of social engineering attacks. Similarly, attention should be paid to implementing proper social engineering awareness to strengthen good security behavior [4]. It is needed to examine other factors that can predict security practices (e.g., self-efficacy, security and privacy concerns, etc.). Research during this field can further be extended to the phenomenon of reverse social engineering, as this field has not been widely reported within the web context. This is particularly necessary, as reverse social engineering allows an attacker to bypass the behavioral detection techniques, thus making attacks easier [2].

VII. CONCLUSION

The steps which are necessary to take while designing defense practices against social engineering include proper security management framework, defining set of goals regarding the security plan and its implementation and periodic risk assessments. Threats don't necessarily represent the same level of intensity for various organizations, so there should be a review of risks of social engineering threats and thus the danger should be rationalized according to the organization type [2]. Social engineering attacks cannot be stopped by using only technology or security systems because it manipulates the users in psychological aspects. These days Cyber-criminals make use of people's fear and anxiety by spreading malicious attachments purporting to provide information and malware via email across the globe. Phishing, vishing, and smishing have grown in frequency and intensity which has increased the chances of losing sensitive information and ransomware attacks in recent times [4].

REFERENCES

[1] KOIDE, Takashi, et al. "To Get Lost is to Learn the Way: An Analysis of Multi-Step SE Attacks on the Web." *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences* 104.1 (2021): 162-181.

[2] Aldawood, Hussain, Tawfiq Alashoor, and Geoffrey Skinner. "Does awareness of SE make employees more secure?." *International Journal of Computer Applications* 177.38 (2020): 45-49.

[3] Lively, Charles. "Psychological based SE." *SANS Institute* (2003).

[4] Alzahrani, Ahmed. "Coronavirus SE attacks: Issues and recommendations." *Int. J. Adv. Comput. Sci. Appl.* 11.5 (2020): 154-161.

[5] Rusch, Jonathan J. "The “SE” of internet fraud." *Internet Society Annual Conference, http://www. isoc. org/isoc/conferences/inet/99/proceedings/3g/3g_2. htm*. 1999.

[6] Gragg, David. "A multi-level defense against SE." *SANS Reading Room* 13 (2003): 1-21.

[7] Ramamoorti, Sridhar. "The psychology and sociology of fraud: Integrating the behavioral sciences component into fraud and forensic accounting curricula." *Issues in accounting education* 23.4 (2008): 521-533.

[8] Salahdine, Fatima, and Naima Kaabouch. "SE attacks: a survey." *Future Internet* 11.4 (2019): 89.

[9] Conteh, Nabie Y., and Paul J. Schmick. "Cybersecurity: risks, vulnerabilities and countermeasures to prevent SE attacks." *International Journal of Advanced Computer Research* 6.23 (2016): 31.

[10] Chargo, Michael A. "You've Been Hacked: How to Better Incentivize Corporations to Protect Consumers' Data." *Transactions: Tenn. J. Bus. L.* 20 (2018): 115.

[11] Libicki, Martin. "Could the Issue of DPRK Hacking Benefit from Benign Neglect?." *Georgetown Journal of International Affairs* 19 (2018): 83-89.

[12] Engebretson, Patrick. *The basics of hacking and penetration testing: ethical hacking and penetration testing made easy*. Elsevier, 2013.

[13] Fan, Wenjun, Kevin Lwakatare, and Rong Rong. "SE: IE based model of human weakness for attack and defense investigations." *International Journal of Computer Network & Information Security* 9.1 (2017).

[14] Mouton, Francois, Louise Leenen, and Hein S. Venter. "SE attack examples, templates and scenarios." *Computers & Security* 59 (2016): 186-209.

[15] Gallegos-Segovia, Pablo L., et al. "SE as an attack vector for ransomware." *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*. IEEE, 2017.

[16] Hadnagy, Christopher. *SE: The art of human hacking*. John Wiley & Sons, 2010.

[17] Mitnick, Kevin D., and William L. Simon. *The art of deception: Controlling the human element of security*. John Wiley & Sons, 2003. // scenarios of prevention

[18] Patel, Naiya. "Social engineering as an evolutionary threat to information security in healthcare organizations." *Jurnal Administrasi Kesehatan Indonesia* 8.1 (2020).

[19] "Top 5 Social Engineering Techniques and How to Prevent Them." Exabeam, 28 Oct. 2020, www.exabeam.com/information-security/social-engineering/. accessed on 8 April 2021

[20]Yates, JoAnne. "MIT Sloan Communication Program Teaching Note by JoAnne Yates, Sloan Distinguished Professor of Management." Web.
https://ocw.mit.edu/courses/comparative-media-studies-writing/21w-732-science-writing-and-new-media-fall-2010/readings/MIT21W_732F10_listening.pdf, accessed on 8 April 2021

[21] Krombholz, Katharina, et al. "Advanced social engineering attacks."*Journal of Information Security and applications* 22 (2015): 113-122.

[22] Heartfield, Ryan, and George Loukas. "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks." ACM Computing Surveys (CSUR) 48.3 (2015): 1-39.

[23] Kotenko, Igor, Mikhail Stepashkin, and Elena Doynikova. "Security analysis of information systems taking into account social engineering attacks." 2011 19th International Euromicro Conference on Parallel, Distributed and Network-Based Processing. IEEE, 2011.

[24] Ivaturi, Koteswara, and Lech Janczewski. "A taxonomy for social engineering attacks."*International Conference on Information Resources Management*. Centre for Information Technology, Organizations, and People, 2011.

[25] Zulkurnain, Ahmad Uways, et al. "Social engineering attack mitigation."*Int. J. Math. Comput. Sci* 1.4 (2015): 188198.

[26] Dorr, Bonnie, et al. "Detecting asks in social engineering attacks: Impact of linguistic and structural knowledge." Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 34. No. 05. 2020.

[27] Irani, Danesh, et al. "Reverse social engineering attacks in online social networks." International conference on detection of intrusions and malware, and vulnerability assessment. Springer, Berlin, Heidelberg, 2011.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 ✆ 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details