IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

SYSTEMATIC REVIEW ON SOCIAL ENGINEERING: HACKING BY MANIPULATING HUMANS

K MADHAVI M. Tech, **Asst. Professor**
Sree Dattha Institute of Engineering & Science, Seriguda, Hyderabad

ABSTRACT

Despite the availability of advanced security software and hardware mechanisms available, still, there has been a breach in the defence system of an organization or individual. Social engineering mostly targets the weakest link in the security system *i.e.* "Humans" for gaining access to sensitive information by manipulating human psychology. Social engineering attacks are arduous to defend as such attacks are not easily detected by available security software or hardware. This article surveys recent studies on social engineering attacks with discussion on the social engineering phases and categorizing the various attacks into two groups. The main aim of this survey is to examine the various social engineering attacks on individuals and countermeasures against social engineering attacks are also discussed.

KEYWORDS

Direct Human Interaction, Phishing, Social Engineering Phases, Preventive Measures

1. INTRODUCTION

Today almost small, medium or large organizations are more concerned about the security of organizational data and information for which they invest a huge amount in developing the most security measure [1]. In an organization, technical vulnerability is not only the cause of cyber-attack. The "Human" is the most vulnerable in the cyber security chain [2]. In recent years humans are being manipulated to extract confidential information and the technique is so-called as "Social Engineering". Social Engineering is a form of art employed by cybercriminals exploiting the psychology of people to gain access or divulge confidential information [3] [4] [5]. Social engineering has a high success rate as compared to other cyber-crime as it exploits the weakest link of the information security system: "the human" [4] [6] [7]. Social engineering attacks are not detected easily by the most advanced security software and hardware as it manipulates the human physiology, not the implemented security mechanism. Some of the popular social engineering attacks in the recent years that mainly targeted the individuals are: Red Pulse attack, 2017: Red Pulse, was the first Initial Coin Offering (ICO) on the NEO (an open platform network for creating decentralized applications). In November 2017, cybercriminals used a fake Twitter account (@RedPulseNEO) to lure victims to a phishing website (redpulsetoken.co), promising to offer an airdrop (free tokens) for a limited period. Asking the victim to enter the private key of their NEO wallet to claim the bonus, criminals stole the victim's funds [8]. Next attack was Fake Twitter Accounts, 2018: Twitter is a popular social media platform within the cryptocurrency community where all-important players of blockchain and digital economy have Twitter accounts. In early 2018, the scammers copied the account of the famous entrepreneur and investor Elon Musk by choosing "Elon Musk" as a display name and

using his profile picture. The scammer also commented on the post of original Elon Mask where they said that they gave away 5000 ETH to Elon's followers where followers should send 0.5 - 1 ETH to his address to participate and get back 5 - 10 ETH. Several followers transferred ETH to the fake addresses. In this attack pretexting was used as a social engineering attack technique [8]. Similarly, next to social engineering attack was Ethereum Classic attack, 2017: In 2017, several people lost thousands of dollars of cryptocurrency after Ethereum Classic website was hacked where the owner of Classic Ether Wallet was impersonated, gained access to the domain registry and then redirected the domains to their servers. Criminals used the user's private key and extracted some of the Ethereum cryptocurrency from the users' wallet [9].

2. LITERATURE REVIEW

[1] examines how social engineering attacks can bypass the world's best security mechanism. The article is a case study where social engineering attacks are performed against a company with their permission to show how the company's sensitive and confidential information could be leaked without breaching the technical security measures. The author emphasizes that organizations must consider the non-technical aspects of security along with strong coordination of technical measures. [10] discusses different social engineering techniques used by attackers. The authors present a basic technical methodology to illustrate one of the social engineering attacks. The article emphasizes on adopting the good practices and measures of handling technology and information for organizations. [11] states that social engineering attacks are the primary threads as it is the entry point for most of the considerable attacks. The authors present different persuasion techniques and theories used by attackers for success of the attacks. The article models game-based analysis techniques to present social engineering attack scenarios. [6] examines the different entities involved in social engineering-based attacks and their relationship. The author presents a conceptual model of social engineering-based attack to find the vulnerable entities in an organization and safeguards mechanism against such attacks. [2] [3] [10] [12] discuss the different attack mechanisms and impact of social engineering attacks and precautions an organization must follow to prevent the attacks. The authors highlight the importance of continuous employee education and awareness programs to prevent attacks effectively. [5] [13] explore the different social engineering attack detection strategies. Both articles discuss two mitigation techniques: Human-based mitigation and Technology-based mitigation techniques to mitigate the social engineering attack within an organization. [14] discusses different types of social engineering attacks and highlight the multi-dimensional approach to defence the social engineering attacks. [15] discusses the preventive solutions, measures, policies, tools and applications required to better recognize the social engineering attacks and prevent such attacks to be successful. [4] presents the different security layers in information security along with defence approaches to mitigate social engineering attacks on respective layers. Also, the article discusses the framework of user characteristics that might affect the user's threat detection capabilities. [7] discusses different social engineering types along with attack channels and demonstrates how online social networks (OSNs) and Cloud Services could be easily used to harvest our personal information for preparation of social engineering attacks. [16] describes how the Software Engineering Attack Detection Model version 2 (SEADMv2) was implemented as an Android application to improves people's ability in detecting malicious social engineering attacks correctly. [17] presents different social engineering scenarios and various tools available that are used in social engineering attacks. It also presents a different recommendation for mitigating social engineering attacks. [18] analyses how Open Source Intelligence (OSINT) data are used to conduct or enhance a social engineering attack against organization/individual with an approach for automated resolution of identification across social media.

Most of the literature focuses on organizational social engineering attacks and presents different preventive and mitigation measures to tackle such attacks particularly on organization/business ignoring the impact of such attacks on individuals. Only a few of them discuss social engineering attacks on individuals/people and recommend some preventive measure against such attacks. [16] primarily focuses on social engineering attacks on an individual by demonstrating how the Android application could be used by an individual to detect social engineering attacks. However, some of the preventive and mitigation measures discussed on [4] [7] [14] [15] [16] [18] are useful and applicable to individuals/persons to prevent and mitigate social engineering attacks. This article discusses how an individual/person is a victim of social engineering attacks and how such attacks could be mitigated and prevented. The rest of the article is organized as phases of social engineering attack are presented in Section 3, Section 4 describes different categories of social

engineering attacks. Prevention & Detection are explored in Section 5. Section 6 presents a Research gap followed by a conclusion in Section 7.

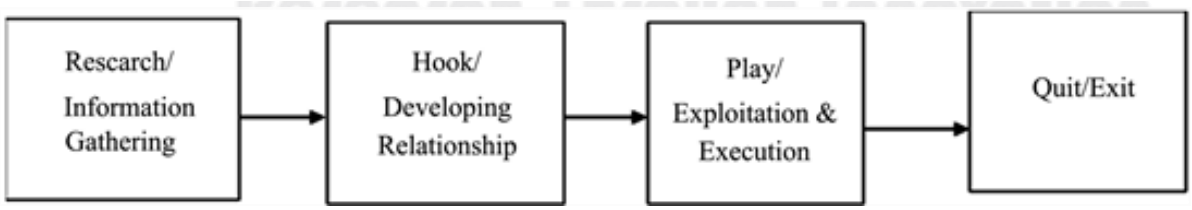
3. PHASES OF SOCIAL ENGINEERING

Social engineering attacks exploit human vulnerabilities to achieve sensitive information, and can happen in one or more steps. Social engineers use the more or less the common pattern to achieve the desired objective, which typically involves four phases [3] [5] [7] [10] [12] [13] [14] [16] [19] [20] [21] [22]: 1) Research: Gathering information about the target; 2) Hook: Maintaining the relationship with the target: 3) Play: Manipulating the information and executing the attack; 4) Exit: Escaping with no any clues. Figure 1 explains the different phases of social engineering attacks discussed in the literature.

In the research/Information Gathering phase, to achieve the purpose of the attack, social engineers investigate, study and gather more information about the target before the actual attack. While this phase is most time-consuming, the likelihood of success also depends on this phase. Social engineers are aware of different information-gathering tools available, software that aid in finding and collecting the data (e.g. Maltego) and use of insignificant data that can be collected either online (e.g. fake website, Facebook, Twitter etc.), over the phone(e. g. impersonation) or in-person (e.g. tail-gaiting, shoulder surfing). Some methods of information gathering require technical skills while others might require the "soft skills" of manipulating human psychology. Social engineers are experts in making a useful picture of the vulnerabilities of a system by combining small pieces of information either gathered from various sources. A major source of information for social engineers is a publicly available source of information, social networking sites (such as personal information, photos, location information, friend's information), dumpster diving, malware, theft and impersonating law enforcement or government agencies. The social engineer looks for some of the target's dressing, greediness, lack of moral duty, awareness level about social engineering and weak policy against attacks. The attacker then analyzes the information gathered and develops an action plan to approach the target. In the next phase, the attacker initiates the communication and tries to develop a relationship with the potential victim through seemingly innocent conversations or email communication. An attacker might start with small conversations and create a situation with the victim's weakness in mind to gain a victim's trust. They might pretend to be a friend, a bank or even government agencies. In the play/exploitation phase the potential target is manipulated or exploited based on the information gathered in previous phases to extract the sensitive information or to compromise the system. An attacker uses a different method of manipulation to bring the target in a desired emotional stage suited to the plan. The victim now starts to provide access to his/her information to an attacker with a feeling of good about giving out the information instead of being guilty about it. Social engineers try to maintain the desired emotional state and continue the communication to an extent so that the target won't get alarmed and contact the agencies. In the exit/quit phase, the attacker either closes the communication slowly or completely with the target. Attackers then erase any clue or proof of the crime, without making the victim know about it.

Figure 1. Social engineering phases.

4. CATEGORIES OF SOCIAL ENGINEERING ATTACK

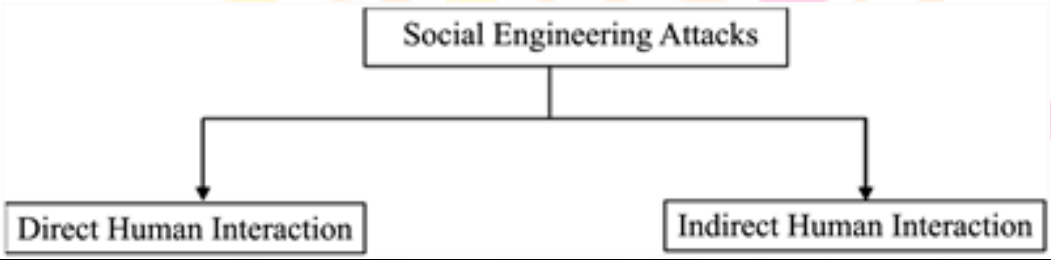


Social engineering attacks are considered as non-technician hacking attacks as most of the attacks are executed without any technical expertise. A social engineer might not have any technical knowledge of hacking or any using any sophisticated tools for executing an attack. Human manipulation is either done in person or using a medium like a phone, email or VOIP. Many literature groups social engineering attacks into different categories. [13] classifies the social engineering attacks into human-based and computer-based. [7] categorized into physical, technical, social and socio-technical approaches. This paper categorized the social engineering attacks into -Direct Human Interaction and Indirect Human Interaction. It is believed this is the simplest way to categorize so it could be understood

and interpreted easily. Also, this paper discusses the countermeasures based on this category. Figure 2 explains the categories of social engineering attacks. This category is according to which the attacker interacts with the target during the attack: direct or indirect.

In Direct Human Interaction, social engineers interact in-person with the target either at the gathering information phase to gather desired information or at exploitation phase where the target is manipulated. Such an attack is usually performed via voice interaction, eye contact or physical contact where limited numbers of victims can be influenced. Such attacks are considered the most dangerous and successful attacks [13]. In Indirect Human Interaction, attackers do not interact directly instead make use of a device like a computer or mobile to collect the desired information and execute the attack. In indirect attacks, social engineers can attack many victims in less time where thousands of emails can be sent to many potential targets or automated calls can be made too many targets at once. Table 1 and Table 2 explain the different types of social engineering attacks discussed in the literature. Table 1 presents some of the popular direct human interaction attack attacks where attackers directly interact with the target during the attack. On the other hand, Table 2 presents the indirect human interaction attacks where attacks are conducted using some software or any other medium.

Figure 2. Social engineering attack category.



Attack type	References	Description
Impersonation	[3] [7] [10] [11] [13] [15]	In such attacks, attackers present a false identity such as an employee or valid user and can gain physical access to the system or network to execute the attack.
Shoulder surfing	[7] [10] [11] [12] [13] [14] [17]	In this type, the attacker observes over the target's shoulders to gather the personal information. Example: observing victim's while entering the password while using ATM, Email or any accounts.
Dumpster diving	[1] [7] [10] [11] [12] [13] [14]	In this attack, the social engineer gathers confidential information from the company's trash or bins. Attacker mostly searches for discarded equipment like old computer materials, drivers, CDs, documents, papers from which they can retrieve confidential data.
Eavesdropping	[10] [12]	It is an act of secretly listening to the communication or conversation of others without their concern. An attacker might use a communication channel like emails or telephone lines to listen to the conversation proactively.
Vishing	[11] [12] [13]	Vishing is known also as phone phishing is where criminals call the victim and persuade them to provide personal, financial or other sensitive information over the phone or perform an action that could handover the confidential information to the attacker. In most cases, voice over internet protocol (VoIP) is used to conduct the vishing attack.

Tailgating	[4] [10] [11] [12] [13]	Tailgating is an act where an attacker gets access to the restricted area, by following someone who has legitimate access to that area. The attacker might ask the victim to hold the door or simply walk in behind a person with security clearance.
Quid pro quo	[2] [4] [13]	Attackers commonly call the target and seduce them by offering free services to solve any technical issues in their network and system. Target then provides the confidential information (Wi-Fi password, username/password) to the attacker assuming the legitimate technical or security personnel.

Table 1. Popular direct human interaction attacks.

Attack types	References	Description
Phishing	[2] [3] [4] [7] [10] [11] [12] [13] [17] [18]	In Phishing, the attacker tries to gain access to confidential information using electronic communication. It is mainly done via emails spoofing. Usually, the victim gets an email from the attackers that appear to come from a legitimate source (like a fellow employee, Credit Card Company, bank etc.) requesting information like social security numbers, bank account number etc.
Baiting	[2] [3] [4] [7] [10] [11] [12] [13]	In this attack, physical medium is used instead of electronic medium like delivery of infected USB drives to employees or leaving physical devices containing malware in a public place to be found by the victim.

Table 2. Popular indirect human interaction attacks.

5. PREVENTION & DETECTION

Social engineering attacks highly depend upon the human errors so prevention of security breaches from such attacks is notoriously difficult. Social engineering attacks are extremely hard and sophisticated to detect even with most advanced security tools. The primary measure to defend against the social engineering attack is to focus on Education, Training and Awareness (ETA) programs for individual and technology implementation. Education, Training and Awareness (ETA) is the primary measure to prevent the social engineering attacks which helps to improve: the safe handling behavior of information, identify the potential attacks, develop the confidence to handle during the attacks. Such information can be delivered via website, TV, radio, newspaper, social media or SMS. Along with the ETA program, an individual should implement different security technology that can prevent and detect the potential social engineering attacks so that they can handle properly once detected. This paper discusses the various countermeasures that exist to stop the attacks: [2] [3] [4] [5] [10] [11] [13] [14] [18] [23] [24] [25].

• Preventive measures at the Information Gathering stage are useful to stop/prevent direct human interaction and indirect human interaction attacks:

○ Do not publish enough information on social media like LinkedIn, Facebook, Twitter, Instagram etc. as such information can be used by a social engineer.

○ Be careful while making use of personal information in a public place like entering the password of an ATM, email or any accounts or having a conversation in person or phone and make sure to log off from all accounts used in public areas (like cybercafe, library etc.).

○ Make sure to erase all data from magnetic media and shred all papers that contain the personal information before they are placed in trash or bin.

• Preventive measures at the Developing Relationship stage differ for direct interaction and indirect interaction attacks:

Countermeasure for direct human interaction attacks are:

○ An unknown person should not be added to the network and individuals should choose Privacy Settings on Social Networking sites that provide the greatest security.

○ Be aware and reject any offer or services from a suspicious person or company and do not rush to open those mail as those might contain the malicious program.

○ Checking the sender's email address before taking any action is highly recommended.

Countermeasure for indirect human interaction attacks are:

○ Not visiting the suspicious site, not opening an email from an unknown person, not sharing the password or system, logging off all accounts when done, making use of a strong password, forwarding the call from outside.

○ Do not install an unauthorized application on mobile/computer devices as they might contain malware.

○ Maintaining software (antivirus, firewall, etc.) up to date is an effective way to prevent social engineering attacks as a social engineer often seeks to determine the unpatched, out of date software that target is using.

• Preventive measures at the Exploitation stage are different for direct interaction and indirect attacks:

Countermeasure for direct human interaction attacks are:

○ Handover of confidential or personal information over the phone, online or in-person must be rejected unless the identity of the person asking the information could be verified.

○ Individuals receiving calls or email of winning the lottery should be aware that they cannot win a lottery or prize that they never entered.

○ Accounts and personal data should be monitored regularly so that you would be aware in case of any attacks.

○ Be aware and suspicious of any email or SMS that develops an environment of emergencies such as email/SMS stating to be arrested if tax is not paid immediately or email/SMS that state some story that requires to be responded to urgently.

Countermeasure for indirect human interaction attacks are:

○ Using two-factor authentication for the accounts, make the account secure even if login credentials are compromised.

○ Always use a different password for each service and create a strong and complex password so that they cannot be guessed easily. Changing password frequently is highly advisable to mitigate the social engineering attacks

○ Some of the indirect human interaction attacks can be detected by implementing tools such as: *Email Gateway*, used to filter out the spam emails that could reduce spam by up to 99.9%, *Anti-Phishing Tools* that connect to a database of the blacklist of phishing website are useful in defense against the phishing attacks, *Robocall and spam call blocking application* like Nomorobo, Hiya Caller ID and Block, RoboKiller, Truecaller, and YouMail Voicemail & Spam Block can be installed on individual mobile that is useful to block telemarketing calls.

• Training on safe behaviour on internet/phone/computer, classifying sensitive information and handling different social engineering attacks should be provided by the government to the public and by the service provider to their customers.

6. RESEARCH GAP

Most of the existing literature presents the social engineering attacks and their countermeasures that target the organizations to breach the defence boundary, manipulating its employees. Although there has been a significant rise in social engineering for organizations and individuals, very few studies have been done on social engineering attacks that targeted the individual/person. The impact of such attacks on individuals has been ignored despite the adverse ramification on financial and mental health of the victim individual. This paper tries to cover the gap by discussing various aspects of social engineering attacks targeted on individuals along with countermeasures to prevent or stop the attacks at different stages of an attack. The countermeasures against attacks differ based upon the category-the direct human interaction and indirect human interaction at various stages of social engineering attack. The countermeasures presented in this paper are useful for both organizations and individuals to fight against the social engineering attacks. The effectiveness of the countermeasures highly depends upon how government and service providers educate, aware and train the public to counter such attacks. Due to lack of proper education, awareness, training and right choice of social engineering detection tools, social engineering attacks targeting the individuals has more success rate than those targeting the organizations as they has strict policy and procedure of access of private information as well as employees are well educated and trained in regular intervals to defence against such attacks.

7. CONCLUSION

The threat of social engineering attack is increasing and will continue to increase in the future. It has been observed that none of the advanced security systems can completely stop the social engineering attacks. Such attacks do not only target the business organization but also the individuals whether they are public or customers of any service provider. It is significant for both individuals and organizations to be aware of different social engineering attacks and follow & implement the prevention, detection and mitigation strategy for the possible. Similarly, the practice of safe information handling behaviour is crucial for every individual to fight against social engineering attacks. To prevent and mitigate the loss of an attack, the government and service providers must adopt a multi-dimensional approach of education, training and awareness program (ETA), proper incident response, effective implementation policy and standard practice for the public and its customers.

REFERENCES

[1] Winkler, I.S. and Dealy, B. (1995) Information Security Technology? Don't Rely on It A Case Study in Social Engineering. 5th USENIX UNIX Security Symposium, Salt Lake City, 5-7 June 1995, 1.

[2] Lohani, S. (2019) Social Engineering: Hacking into Humans. International Journal of Advanced Studies of Scientific Research, 4.

[3] Kumar, A., Chaudhary, M. and Kumar, N. (2015) Social Engineering Threats and Awareness: A Survey. European Journal of Advances in Engineering and Technology, 2, 15-19.

[4] Kaushalya, S.A.D.T.P., Randeniya, R.M.R.S.B. and Liyanage, A.D.S. (2018) An Overview of Social Engineering in the Context Of Information Security. 2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS), Bangkok, 22-23 November 2018, 1-6.

[5] Zulkurnain, A.U., Hamidy, A.K.B.K., Husain, A.B. and Chizari, H. (2015). Social Engineering Attack Mitigation. International Journal of Mathematics and Computational Science, 1, 188-198.

[6] Chitrey, A., Singh, D., Bag, M. and Singh, V. (2012) A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model. International Journal of Information & Network Security, 1, 45-53.

[7] Krombholz, K., Hobel, H., Huber, M. and Weippl, E. (2015). Advanced Social Engineering Attacks. Journal of Information Security and applications, 22, 113-122.

[8] Weber, K., Schütz, A.E., Fertig, T. and Müller, N.H. (2020). Exploiting the Human Factor: Social Engineering Attacks on Cryptocurrency Users. In: Zaphiris, P. and Ioannou, A., Eds., Learning and Collaboration Technologies. Human and Technology Ecosystems. HCII 2020. Lecture Notes in Computer Science, Springer, Cham, 650-668.

[9] Brook, C. (2017) Classic Ether Wallet Compromised via Social Engineering. https://threatpost.com/classic-ether-wallet-compromised-via-social-engineering/126657/

[10] Breda, F., Barbosa, H. and Morais, T. (2017) Social Engineering and Cyber Security. Proceedings of the International Conference on Technology, Education and Development, Valencia, 6-8 March 2017, 4204-4211. http://dx.doi.org/10.21125/inted.2017.1008

[11] Yasin, A., Fatima, R., Liu, L., Yasin, A. and Wang, J. (2019) Contemplating Social Engineering Studies and Attack Scenarios: A Review Study. Security and Privacy, 2, e73. https://doi.org/10.1002/spy2.73

[12] Parthy, P.P. and Rajendran, G. (2019) Identification and Prevention of Social Engineering Attacks on an Enterprise. 2019 International Carnahan Conference on Security Technology, Chennai, 1-3 October 2019, 1-5. https://doi.org/10.1109/CCST.2019.8888441

[13] Salahdine, F. and Kaabouch, N. (2019) Social Engineering Attacks: A Survey. Future Internet, 11, 89. https://doi.org/10.3390/fi11040089

[14] Luo, X., Brody, R., Seazzu, A. and Burd, S. (2011) Social Engineering: The Neglected Human Factor for Information Security Management. Information Resources Management Journal, 24, 1-8. https://doi.org/10.4018/irmj.2011070101

[15] Aldawood, H. and Skinner, G. (2018) Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal. 26th International Conference on Systems Engineering, Sydney, 8-20 December, 1-6. https://doi.org/10.1109/ICSENG.2018.8638166

[16] Mouton, F., Teixeira, M. and Meyer, T. (2017) Benchmarking a Mobile Implementation of the Social Engineering Prevention Training Tool. 2017 Information Security for South Africa, Johannesburg, 16-17 August 2017, 106-116. https://doi.org/10.1109/ISSA.2017.8251782

[17] Osuagwu, E.U., Chukwudebe, G.A., Salihu, T. and Chukwudebe, V.N. (2015) Mitigating Social Engineering for Improved Cybersecurity. 2015 International Conference on Cyberspace, Abuja, 4-7 November 2015, 91-100. https://doi.org/10.1109/CYBER-Abuja.2015.7360515

[18] Edwards, M., Larson, R., Green, B., Rashid, A. and Baron, A. (2017) Panning for gold: Automatically Analysing Online Social Engineering Attack Surfaces. Computers & Security, 69, 18-34. https://doi.org/10.1016/j.cose.2016.12.013

[19] Abdalla, I. (2018) Social Engineering Threat and Defense: A Literature Survey. Journal of Information Security, 9, 257-264. https://doi.org/10.4236/jis.2018.94018

[20] Francois, M., Mercia, M., Louise, L. and Venter, H.S. (2014) Social Engineering Attack Framework. 2014 Information Security for South Africa, Johannesburg, 13-14 August 2014, 1-9. https://doi.org/10.1109/ISSA.2014.6950510

[21] Social Engineer. The Social Engineering Framework. https://www.social-engineer.org/framework/information-gathering/

[22] Hoxhunt. Social Engineering—What Is It and How to Prepare for It? https://www.hoxhunt.com/blog/social-engineering/

[23] Thompson, S.T.C. (2006) Helping the Hacker? Library Information, Security, and Social Engineering. Information Technology and Libraries, 25, 222-225. https://doi.org/10.6017/ital.v25i4.3355

[24] Hitachi Systems (2019) 10 Ways Businesses Can Prevent Social Engineering Attacks. https://www.hitachi-systems-security.com/blog/10-ways-businesses-can-prevent-social-engineering-attacks/

[25] Whitney, L. (2020) How to Block Robocalls and Spam Calls. https://au.pcmag.com/apple-iphone-x/57316/how-to-block-robocalls-and-spam-calls