 doi:10.20944/preprints202207.0054.v1

Article

Social Engineering: Concepts, Techniques, and Security Countermeasures

Maria Ul Aziz

University of Bradford, Bradford, United Kingdom
m.i.ulazizparveen@bradford.ac.uk

Abstract: This research paper describes the social engineering concepts, techniques, and security countermeasures. This research aims to study various social engineering techniques to find the best countermeasures that would help to reduce social engineering attacks.

Keywords: social engineering; security countermeasures; security awareness; security policies

1. Introduction

For the past few years, there has been a huge improvement in the security tools, and it has become challenging for hackers to hack the information by using technical resources only. Therefore, rather than just relying on technical resources to gain unauthorised access to information the hackers have been using social engineering techniques. Social engineering is a non-technical method of stealing information (Ivaturi and Janczewski, 2011).

Social engineering refers to making use of human behaviour to gain access to their information. Regardless of using security measures such as firewalls, intrusion detection systems or anti-virus software; social engineering can still be challenging because the hackers target humans directly rather than machines. As humans tend to trust other humans easily and consequently can get deceived by them as well (Salahdine and Kaabouch, 2019). Hackers use different deception tricks and play with human psychology to make people trust them. As hackers can get more information directly from humans than using any other technical means and attacking the machines, therefore, this technique has been increasing rapidly. And to reduce social engineering attacks it is important to know the techniques which hackers use and the security measures that can be taken to keep the information protected. This research includes different social engineering techniques and security countermeasures. And how these measures can be implemented in the organisations to ensure the security of their information.

Research questions:

Social Engineering is a broad topic and there can be a lot of research done. But this research paper will mainly focus on these three questions:

What makes social engineering successful?
What techniques social engineers are using?
Which is the best way to reduce social engineering attacks?

2. Social engineering

In the literature, the researchers have been providing different definitions for the term 'Social Engineering Attacks' but all these definitions have the same broad concept. Conteh et al, described social engineering as 'Human Hacking' an art that tricks employees and consumers, and they end up disclosing their credentials and then the hackers use this information to gain access to their network and accounts (Conteh and

 doi:10.20944/preprints202207.0054.v1

Schmick, 2016). Engebretson defined social engineering as "One of the simplest methods to gather information about a target through the process of exploiting a human weakness that is inherited by every organization" (Engebretson, 2013).

Ghafir et al defined social engineering as "A breach of organizational security via interaction with people to trick them into breaking normal security procedures" (Ghafir et al., 2016).

In the last couple of years, the social engineering attacks have increased rapidly as almost all businesses have moved to the digital landscape. Also, the attackers are taking advantage of the current COVID-19 pandemic and targeting people with fake support messages or claiming to be calling from vaccination centres and gaining their sensitive information. According to a report by PurpleSec, there was a 667% increase in the spear-phishing emails during Covid and Google reported in April 2020 that it has blocked 18 million daily malicious malware and phishing emails and 240 million daily spam messages related to covid (Mashtalyar et al., 2021).

What is making the social engineering attacks successful? There can be many reasons behind this depending on the attackers' targets. If the targets are common people, then the main reason can be a lack of awareness about social engineering attacks. As humans are considered the weakest link in the security chain and most of the research community agrees on this as well (Ghafir et al., 2016). Therefore, to stay protected from social engineering attacks it is crucial to work on humans. Provide them with good knowledge of this security issue, its impacts and the measures that can be taken to reduce these social engineering attacks.

3. The motivation behind social engineering attacks

Social engineers carry out these attacks for various motives such as economic, and financial profit, personal interest, and political reasons. The information that social engineers gain from these attacks can be used for various reasons, if the purpose of the attack is to gain financial profit, then the attackers can trade this information to the competitors of that organisation or sell this information on the dark web. But some social engineers carry out these attacks out of curiosity about that organisation or just to challenge themselves and use new techniques. Another reason that motivates someone to carry out these attacks can be personal grudges; someone who might want to take revenge or an old employee who got dismissed from the job can try social engineering techniques to bring the company's reputation down. This type of attack is often successful because the old employee will already have some sensitive information about the company that will assist him in carrying out the attack. Social engineering can also be used to gain political interest. One political party can try social engineering attacks to gain sensitive information about the opposition and can use this information against them to bring their reputation down (Chizari et al., 2015).

4. Social engineering attack strategies

Social engineering is a growing threat and attackers are using various techniques to make these attacks successful. But most of these attacks follow a common pattern. And this pattern has been classified into four phases by Malcolm Allen. These four phases can be referred to as the social engineering cycle. These phases are Information gathering, Relationship development, Exploitation, and Execution (Chizari et al., 2015). Jassen described these phases in a series of four steps, which are: Global information gathering, specific information gathering, gaining access to information systems, and realizing the final goal (Oosterloo, 2008). By evaluating these approaches Oosterloo defined another model which combines the main focuses of both approaches, which are developing the relationship and obtaining information. And the model defined by Oosterloo has these four phases:

(Oosterloo, 2008)

1. Preparation

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 July 2022 doi:10.20944/preprints202207.0054.v1

2. Manipulation
3. Exploitation
4. Execution

In this research paper these four phases will be described and the techniques that are used in each of these phases.

Preparation: In the first phase all the target information is collected. Social engineers try to collect as much information as they can by using different techniques. Some most common techniques that are used by attackers are physical reconnaissance, dumpster diving and forensic analysis, phreaking, phishing, and profiling. All these techniques are used to gather information about virtual and physical attributes which assists in the next phases (Oosterloo, 2008).

Manipulation**:** In this phase of social engineering attack the attackers try to manipulate the target by using various techniques, particularly psychological tactics. As humans tend to trust other humans easily and these chances increase when someone is in need. And therefore, the social engineers take advantage of this human nature to manipulate them and develop a relationship to get their trust and if this phase gets successful it becomes easy for the attackers to carry on the next phase of the attack. The attackers use psychological tactics such as the use of authority and reverse social engineering techniques to manipulate victims (Oosterloo, 2008).

Exploitation: This phase has a strong link with the previous phase because in this phase the social engineers get the advantage of the trust they developed with the victim and obtain sensitive information. Some of the techniques that can help in this phase are Tailgating, Piggybacking, Desk sniffing/office spoofing and Item dropping (Oosterloo, 2008).

Execution: This is the final phase in which the attackers use all the gathered information from the previous phases and carry out the attack. (Oosterloo, 2008). The results of this phase depend on the intentions of the attackers and what they want to obtain from this attack. This phase does not only consist of social engineering, but it also allows attackers to carry more attacks on the compromised system. Once the attackers have access to the system, they can download malicious code on it.

5. Social engineering techniques

Social engineering techniques can be classified into different categories. In this research paper, the social engineering taxonomy proposed by Krembholz et al. will be used. This taxonomy has been illustrated in fig 1.

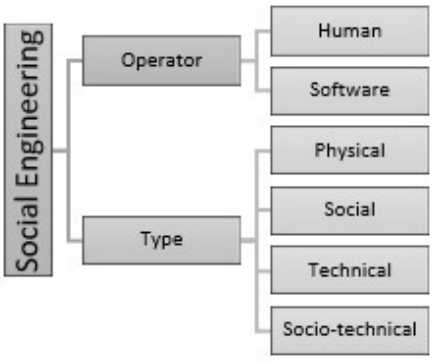

Figure 1. Social Engineering taxonomy.

Based on the operator the social engineering attack techniques can be classified into two categories: Humanbased attacks and Software-based attacks (Krombholz, 2015).

Human-based: **Human-based** attack means the attacks that are conducted in person. It is easy to gain access to sensitive information through humans than computers thus,

 doi:10.20944/preprints202207.0054.v1

these attacks are successful. But because these attacks are conducted in person and therefore, compare to software or computer-based attacks the number of targets in humanbased attacks is limited (Krombholz, 2015). Types of Humanbased attack techniques can be shoulder sniffing, persuading or dumpster diving (Aldawood and Skinner, 2020).

Software-based: These attacks are conducted using automated software. A software engineering tool kit is an example that can be used to carry out spear-phishing email attacks. With software-based attacks, a large number of attacks can be carried out in a short time (Krombholz, 2015). Furthermore, social engineering techniques can be classified into four different types: Physical, Social, Technical, and socio-technical.

Physical: As the name indicates, in this type of approach the attackers have to perform some physical activities to gain the victim's information. Examples of this can be tailgating and dumpster diving (Aldawood and Skinner, 2020).

Social: Social based techniques are the most effective techniques to carry out social engineering attacks. The attackers use different socio-psychological techniques to build relationships with victims and manipulate them. These techniques can include the use of authority or methods to impress the victim and gain information (Krombholz, 2015). This type of technique is mainly used in the second phase of the social engineering attack as the purpose is to build a relationship with the victim.

Technical: This method uses technical tools to gain information. The attackers can attack different networking websites with less security to steal sensitive information. Examples of these attacks can be pop-up windows, email attachments or ads on the websites (Aldawood and Skinner, 2020).

Socio-technical: The combination of both social and technical attacks can be used to carry out effective and successful social engineering attacks. As the social method will help to build a relationship with the victim and gain trust, the technical method can be used to gain sensitive information from technical means. Spear-phishing and baiting is the example of socio-technical attack techniques (Aldawood and Skinner, 2020).

Some commonly used social engineering techniques:

Physical Reconnaissance: Social engineers use this technique to gather information about their victims. They can use different tactics such as shoulder surfing or eavesdropping to gain information (Oosterloo, 2008). This is a physical social engineering technique and is used in the first phase of the attack.

Phishing: Phishing is a commonly used social engineering technique. It is the process in which the attackers send messages or emails containing malicious content, but they make it look like they came from legitimate and trustworthy sources. The phishing emails and messages normally contain website links that direct victims to the website with malicious scripts (Aldawood and Skinner, 2020).

Spear-phishing: Unlike phishing, spear-phishing targets a specific individual. The message sent to the victim includes the information familiar to him. The attackers do this attack after doing proper research about the victim and making the message look like it came from an authentic source (Aldawood and Skinner, 2020).

Reverse Social engineering: The social engineer makes such circumstances that the victim himself access the social engineer. The victim request help from the social engineer and the social engineer helps the victim in such a way that assist him to carry out the attack (Watson et al, 2014).

Baiting: In this attack, the attacker uses a storage device e.g., a USB drive with malware already downloaded on it. And intentionally leaves it somewhere to be found by the victim. And when found, out of curiosity the victim inserts that device into his computer system and the system gets compromised without his knowledge (Breda et al., 2017).

Tailgating: Tailgating is a type of physical social engineering attack. In tailgating, the attackers try to get into the building. As the companies use access cards or identity cards to get access into the building but attackers follow the person who has the access and when that person sees someone coming after him, in courtesy that person might hold the door for the one coming after him (attacker) and this way the attacker can easily get into

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 July 2022 doi:10.20944/preprints202207.0054.v1

the building. (Aldawood and Skinner, 2020). Or even if that person does not hold the door the attacker will try to enter before the door closes.

Dumpster diving and forensic analysis: Dumpster diving is the process of finding sensitive information by going through the company's trash and checking the discarded documents (Alharthi and Regan 2020) Similarly forensic analysis is the process of finding information by analysing discarded computer equipment such as hard drives and memory sticks (Oosterloo, 2008).

6. Security countermeasures

Social engineering attacks are one of the trickiest attacks to prevent as they include the use of technology as well as social techniques. Therefore, to reduce these attacks along with technical security, physical security and social awareness should be used. Based on the research done for this paper, some security countermeasures that can be used to prevent social engineering techniques are explained below:

Physical security: Physical security is required to prevent human-based social engineering attacks. The companies should make sure that they have set up certain security that will not allow an unauthorised person to access the building. But at the same time, these measures should not be complex enough to interrupt the authorised person's access. For example, the companies can use barriers where only one person is allowed to pass at a time and with an identification card or to make it more secure to use biometrics (Oosterloo, 2008). The use of biometric identification is better than identity cards because with identification cards the social engineer can use the excuse that he left his card home or lost it and then gain access using the temporary card. This security measure is useful to prevent attacks such as tailgating. But this security measure will only prevent the external social engineers. If the social engineer is from within the company, then this measure would not help. Therefore, further security is necessary to implement.

Security Policies and procedures: The security of the company also includes having certain policies set to ensure the security of the company. For example, the companies can have a password policy which requires the users to include special characters, lower- and upper-case letters and numbers in the password. And prompt users to change their password after a certain time limit. And there should be a policy of wearing the ID card all the time in the company. Some other policies such as restricting the employees to bin the documents with sensitive information should be implemented to prevent dumpster diving attacks (Ghafir et al., 2016). The companies can also set physical access rules to certain areas within the building as well as limit access to virtual information. For example, there should be a different department of people having access to certain areas and information. Particularly limit the information accessible from the help desk. Because help desks are the first point of interaction and therefore, the information accessible to them should be limited. So that even if the attacker manages to manipulate the employee at the help desk, he should not be able to access any sensitive information.

Awareness and training: Another way to reduce the social engineering attacks is to spread the awareness and train the employees to tackle these attacks. The employees should be given good training and awareness programs should be conducted to educate employees on social engineering techniques and tools. These awareness programs can include conferences and awareness campaigns. And the training can include workshops, lectures, or virtual labs (Mashtalyar et al., 2021). And the companies should arrange a session after a couple of weeks or whenever any new attack occurs. To educate employees about the latest attacks. Even if the attack did not occur in that company or did not get successful but still the employees should be aware of it.

 doi:10.20944/preprints202207.0054.v1

7. Discussion and future work

Social engineering is a serious concern for organisations. As social engineering attacks are increasing organisations must implement strong security rules to keep their information secure from attackers. In this research paper, social engineering techniques and security countermeasures were discussed.

The main questions of this research paper will be discussed in this section. By researching the techniques used by social engineers such as phishing, tailgating, baiting and reverse social engineering the reason for the successful social engineering attacks can be known. In all these techniques the attackers try to deceive people directly or indirectly. The successful attacks can be because of two main reasons; the people not paying attention to details this can be because of the lack of awareness and the second is weak security policies in the company. if the target of the attacker is the endpoint user, then it is easy for the attacker to gain information from him than to get information from someone within the organisation. As common people easily trust other people and consequently, give the attackers sensitive information. For attackers, any information related to the victim is important, even if the victim thinks that information is not sensitive.

Organisations' weak security causes successful social engineering attacks. Attacks such as tailgating can be mitigated by having strong physical security. And attacks like dumpster diving and forensic analysis can be reduced by implementing strong security policies.

Which is the best way to reduce social engineering attacks? when I started research on social engineering, I came across this statement which Ian Mann the author of the book 'Hacking the Human' mentions in his book that he does not agree with the statement that was published in an article that the attackers take advantage of the people's naivety and education is the only way to prevent social engineering attacks (Mann, 2008).

As I researched the techniques such as phishing, spearphishing, dumpster diving and baiting I disagreed with Ian Mann. But as I further researched other techniques such as tailgating, piggybacking and the research about security countermeasures made me disagree with the statement that was published in the article mentioned by Ian.

I believe one best way of reducing attacks cannot be chosen. The awareness of the attacks is as important as the security policies. Even if the company has strong security policies but its employees have less awareness about the attacks then it can still be harmful. For example, if the company's policy is to not bin the sensitive information but some employees can still do it which can cause successful dumpster diving. And similarly, even if the employees are well trained, they cannot completely keep the information secure from the attackers. Therefore, policies such as limited information access should be implemented. For future work, more research should be done on technical security and how to implement stronger security policies.

References

[1] Ivaturi, K. and Janczewski, L., "A Taxonomy for Social Engineering attacks" (2011). CONF-IRM 2011 Proceedings. 15. http://aisel.aisnet.org/confirm2011/15

[2] Breda, F., Barbosa, H. and Morais, T., 2017.SOCIAL ENGINEERING AND CYBER SECURITY. 4204-4211. 10.21125/inted.2017.1008.

[3] I. Ghafir and V. Prenosil, "Malicious File Hash Detection and Drive-by Download Attacks," International Conference on Computer and Communication Technologies, series Advances in Intelligent Systems and Computing. Hyderabad: Springer, vol. 379, pp. 661-669, 2016.

[4] Venkatesha, S., Reddy, K. and Chandavarkar, B., 2021. Social Engineering Attacks During the COVID-19 Pandemic. SN Computer Science, 2(2).

[5] I. Ghafir, V. Prenosil, J. Svoboda and M. Hammoudeh, "A Survey on Network Security Monitoring Systems," International Conference on Future Internet of Things and Cloud, Vienna, Austria, pp. 77-82, 2016.

[6] Mann I. Hacking the Human: Social Engineering Techniques and Security Countermeasures. Aldershot: Gower; 2008.

[7] Ghafir, I., Prenosil, V., Alhejailan, A. and Hammoudeh, M., 2016. Social Engineering Attack Strategies and Defence Approaches. 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud),.

[8] Conteh, N. and Schmick, P., 2016. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), pp.31-38.

[9] I. Ghafir, V. Prenosil, A. Alhejailan and M. Hammoudeh, "Social Engineering Attack Strategies and Defence Approaches." International Conference on Future Internet of Things and Cloud. Vienna, Austria, pp. 145-149, 2016.
[10] Engebretson, P., 2013. The basics of hacking and penetration testing. 2nd ed. Amsterdam: Syngress, an imprint of Elsevier.
[11] Salahdine, F. and Kaabouch, N., 2019. Social Engineering Attacks: A Survey. Future Internet, 11(4), p.89.
[12] I. Ghafir, V. Prenosil, and M. Hammoudeh, "Botnet Command and Control Traffic Detection Challenges: A Correlation-based Solution." International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 7(2), pp. 27-31, 2017.
[13] Chizari, H. & Zulkurnain, A. & Hamidy, A. & Husain, A., (2015). Social Engineering Attack Mitigation. International Journal of Mathematics and Computational Science. 1. 188-198.
[14] I. Ghafir, J. Saleem, M. Hammoudeh, H. Faour, V. Prenosil, S. Jaf, S. Jabbar and T. Baker, "Security Threats to Critical Infrastructure: The Human Factor," The Journal of Supercomputing, vol. 74(10), pp. 1-17, 2018.
[15] Oosterloo, B., 2008. Managing social engineering risk: Making social engineering transparant (Master's thesis, University of Twente).
[16] Aldawood, H. & Skinner, G. (2020). An Advanced Taxonomy for Social Engineering Attacks. International Journal of Computer Applications. 177. 975-8887. 10.5120/ijca2020919744.
[17] I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han and R. Hegarty, K. Rabie and F. J. Aparicio-Navarro, "Detection of Advanced Persistent Threat Using Machine-Learning Correlation Analysis," Future Generation Computer Systems, vol. 89, pp. 349-359, 2018.
[18] Odeh, N., Eleyan, D. and Eleyan, A., 2021. A SURVEY OF SOCIAL ENGINEERING ATTACKS: DETECTION AND PREVENTION TOOLS. Theoretical and Applied Information Technology, 99(18).
[19] Alharthi D.N., Regan A.C. (2020) Social Engineering Defense Mechanisms: A Taxonomy and a Survey of Employees' Awareness Level. In: Arai K., Kapoor S., Bhatia R. (eds) Intelligent Computing. SAI 2020. Advances in Intelligent Systems and Computing, vol 1228. Springer, Cham.
[20] I. Ghafir, V. Prenosil, M. Hammoudeh, T. Baker, S. Jabbar, S. Khalid and S. Jaf, "BotDet: A System for Real Time Botnet Command and Control Traffic Detection," IEEE Access, vol. 6, pp. 1-12, 2018.
[21] Bullée, J. and Junger, M., 2019. Social Engineering. The Palgrave Handbook of International Cybercrime and Cyberdeviance, pp.1-28.
[22] Krombholz, K., Hobel, H., Huber, M. and Weippl, E., 2015. Advanced social engineering attacks. Journal of Information Security and Applications, 22, pp.113-122.
[23] Trim, P. and Upton, D., 2016. Cyber security culture: counteracting cyber threats through organizational learning and training.
[24] Mashtalyar, N., Ntaganzwa, U., Santos, T., Hakak, S. and Ray, S., 2021. Social Engineering Attacks: Recent Advances and Challenges. HCI for Cybersecurity, Privacy and Trust, pp.417-431.
[25] Watson, G., Ackroyd, R. and Mason, A., 2014. Social engineering penetration testing. Waltham, MA: Syngress.
[26] M. Lefoane, I. Ghafir, S. Kabir, and I. Awan, "Machine Learning for Botnet Detection: An Optimized Feature Selection Approach". International Conference on Future Networks & Distributed Systems. Association for Computing Machinery, New York, NY, USA, 2021.
[27] S. Eltanani and I. Ghafir. "Coverage Optimisation for Aerial Wireless Networks." 2020 14th International Conference on Innovations in Information Technology (IIT). IEEE, 2020.
[28] I. Ghafir, V. Prenosil, M. Hammoudeh and U. Raza, "Malicious SSL Certificate Detection: A Step Towards Advanced Persistent Threat Defence," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.
[29] J. Svoboda, I. Ghafir, V. Prenosil, "Network Monitoring Approaches: An Overview," International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 5(2), pp. 88-93, 2015.
[30] I. Ghafir and V. Prenosil. "Proposed Approach for Targeted Attacks Detection," Advanced Computer and Communication Engineering Technology, Lecture Notes in Electrical Engineering. Phuket: Springer International Publishing, vol. 362, pp. 73-80, 9, 2016.