Social Engineering, New Era Of Stealth And Fraud Common Attack Techniques And How To Prevent Against

Asma A. Alsufyani, Lama A. Alhathally, Bayan O. Al-Amri, Sabah M Alzahrani

Abstract: as our modern daily lives require continues connection to online resources and services, the threat of these services being exploited to do harm rapidly increases. The human naïve nature could be a reason to that whereas some threats and attacks are actually the absolute opposite of such a trait, human minds can produce both good and bad methods to use technology, one of the very bad methods nowadays is widely known as social engineering, an evidence to prove that internet cannot and won't be a safe place for those who don't carry a careful and wise practice while using technology. This survey paper addresses social engineering threats and categories and, discuss some of the studies on countermeasures to prevent such attacks, providing a comprehensive survey study of social engineering to help understand more about this modern way of theft, manipulation and fraud.

Index Terms: Baiting; Dumpster Diving; Eavesdropping; Phishing; Pretexting; Quid Pro Quo; Reverse Social Engineering; Security Threats; Shoulder Surfing; Social Engineering; Watering Hole.

1 INTRODUCTION

Exploiting systems and software vulnerabilities with IT knowledge and techniques using programming and malicious software usually referred to as hacking, however, exploiting human simplicity and weaknesses to perform cybersecurity attacks is known as SOCIAL INGINEERING. As author [1] described social engineering as an art of penetrating cybersecurity by exploiting human psychological approach without a clear notice from the victim to be prepared against such threats or attacks. Technology development has reached a point where almost every individual and facility are using it, due to the huge benefits technologies provide to societies and businesses in every aspect of daily life, social networking, educational, medical, military systems, and many more systems, are all profiting from what technology is offering, yet these benefits come with risks where malicious acts could use them for undesirable purposes, with this growing unstoppable interest and connection with the cyber world, many vulnerabilities are starting to expose these systems to the threats of adversaries and by lots of methods, including social engineering, which in fact it may not need much of computing expertise to practice against these vulnerabilities and actually make a damage [2]. This type of attacks focuses mostly on manipulating the human minds by tapping on some natural traits like emotions, interests, self-indulgence, foolishness, boredom, and innocence [3], [2].

- *Asma A. Alsufyani, currently doing a master's degree in Cybersecurity, Taif University, Saudi Arabia. E-mail: asma.msufyani@gmail.com*
- *Lama Alhathally, currently is pursuing master's degree in Cybersecurity, Taif University, Saudi Arabia. E-mail: lamoshalh@gmail.com*
- *Bayan O. Al-Amri, a master's degree student in Taif University majoring cyber security, E-mail: bayan.o.amri@gmail.com*
- *Sabah M. Alzahrani, assistant professor in computer science, Taif University, E-mail: sa.sabah@tu.edu.sa*

It is a well-known fact among information security researchers that the human element represents one of the weakest vulnerabilities in the security system, attackers taking advantages of this point through performing social based methods to attack instead of depending on software alone has become a key danger that faces cyber security [4]. It takes a really smart person to perform such malicious attacks, combining intelligence and other elements together to achieve a successful attack can take up to months of preparation, or simply in just a matter of a click by someone who lacks awareness and Information security knowledge, or who simply fell under a mindless mistake. Social engineering Attackers usually need three elements to help them perform a successful attack, in figure 1, the elements are[4]:

Figure 1 *the three elements attacker need in social engineering*

- **Technique**: what can they use and the way it'll be used along with talents.
- **Chances**: the perfect timing and entrée to begin the attack.
- **Purpose**: the trigger and cause for such a malicious act[4].

It almost seems like a game that an adversary plays on his/her victims, for example like deceiving and manipulating the simple good willing people, those who are offering a hand of help without making sure about the facts, that attacker could plot a scenario about a friend that needs urgent help, figuring ways to reach a valuable assets like data or gaining unauthorized access using such deception [5]. A study conducted in 2012[6] about what triggers a person to perform

a social engineering attack, showed that the main reason was the desire to obtain a restricted information, and comes after it in order intentions such as economic expansion, seeking benefits, self-entertainment, and paybacks for grudges, then followed by unspecified other reasons [6], [7]. On the other side, victims of this sort of attacks also are categorized based on the reasons why they fall for social engineering attacks, researchers stated that it's because of the good willing first judgment impressions, that it makes it hard to discover malicious intents, in other words, victims are unaware of the actual results of their actions, unaware of the damages that flaws can cause, users are more likely to act recklessly in a dangerous way, plus they lack a good communal background or experience [8], [9], [10], [11].

In our survey paper,s we are going to discuss various social engineering techniques and some countermeasures to prevent them, in BACGROUND we will address the common strategies, situations where such attacks performed. Next, we are going to discuss the types of THREATS social engineering present, then we will argue some possible COUNTERMEASURES against social engineering attacks, lastly there will be a discussion about the topics we addressed in the paper in fair brief details.

2 BACKGROUND

As stated in an article issued in CPNI, SE is described through a several establishments and individuals depend on mental and safety circumstances. Some stated that it's a "breach an establishment's safety through communications with individuals". Moreover, Keven Mitnick (a former intruder who was registered in FBI as the utmost requested criminal) defines it as "exploiting of individuals simplicity through effect, persuading and manipulating to gain an important info". In addition, it can be defined as a talent that used by anonymous person to gain trust that lead the attackers to enter the establishment through an employee. As a result, the attackers can modify the establishment policies and gain the entrée pass to the establishment data [12]. Social engineering fundamentally involves manipulation of individuals mentally and emotionally to obtain secret or valuable establishment data as user IDs, passwords, or company folders from unsuspicious workers [12]. There are various individual or technological method which intruders can acquire the information from phishing attack or searching the trash in a certain way then exposed it or take advantage of these data. Most professional intruders take advantage of people and technology to have an entree to the establishment resources. There are a several strategies to perform Social engineering intrusion which are [13]:

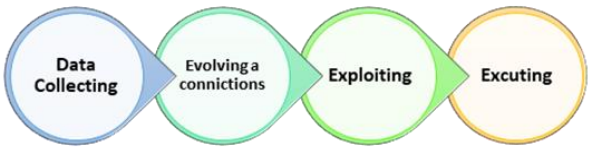


Fig. 1: 1: *The strategies of social engineering, Adapted from N. Y. Conteh and P. J. Schmick [13].*

1. The data collection procedure acquires info from well-known source such as web pages, social network, phone book from a previous social engineering attack [12].
2. Stage 2 is to utilized info to evolve a common connection with the victim [12].
3. Stage 3 exploit the evolving connection stage to create a profile about the victim [12].

The way Social engineering functioning

Social engineering is illustrated as a "non-technological way of attack that depend on person's communication and frequently contains deceiving other persons to breach usual security actions" [14].

Popular Social Engineering Situations Contain

- **Worker Data:** Files that include personal info about worker's names, departments and so on, are vital because it used throughout the physical pen test to check that info is authenticated. The knowledge of confidential data as internal lead to seem as somebody authenticate [14].

- **Emails**: In Emails business emails and from other sources similar to LinkedIn, official website can be found regularly. However, documents comprising a few email addresses that helps to find, realize inner data and the email addresses in the company [14].

- **Directed Documents:** these types of documents could assist pen test performer to make fakes of the papers. This is crucial for social engineering meeting because it tricks the workers to do the act which you need [14].

- **Bills:** Bills reveal corporation's customers and associate's data. This information helpful for pen test performer and make use of these data to pretend to be as a worker from the targeted corporation this will lead them to enter the corporate structure [14].

- **IDs and PINs:** usually several business staffs retain their IDs and PINs in pasty small papers. This small part of info usually could find in the trash as managers are imposing PINs to alter throughout short time like every two or three months. This will lead to discover and reveal the erected pattern of IDs and PINs and with might one of them is currently used [14].

- **Electronical Media:** USBs, CDs and DVDs disks even hard drives could find in the trash. These could gather and analyze. Frequently people throw it without erase its content or destroys it so it's very easy to retrieve it and used it to gain a corporation confidential data [14].

- **Handbook, Manual and Operational Actions:** Manual and handbooks usually find it in the corporation garbage. Furthermore, these files renew frequently, and the old forms have no need. Generally, these forms have an enormous amount of info about inner procedures and systems that could take their individual part in the communicating [14].

- **Signs:** Documents that have signs particularly from approved individuals similar to business leader, Head of

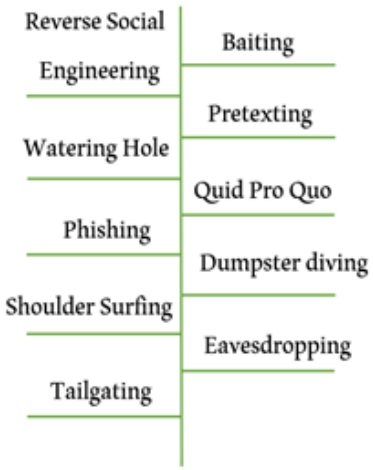
branches and Account Administrators are significant because their sign could imitate and forge which could apply in diversity of situations as a legal approval file [14].

3 SOCIAL ENGINEERING THREATS

In social engineering, an attack come in different ways: on an email message, over phone calls or by pretending as a trusted entity. The phone used to make the verification process of entity difficult. For the same reason the email is used, and it also makes the impersonating process so easy. The social engineering threats can classify in many forms: one of these forms classified the social engineering threats into human and physical, another form classified it into technical, social and physical, and a third one classified it into direct and indirect [15]. In our paper, we will list the threats without any classification. We will display some social engineering threats that can exploited by attackers to get some benefits:

3.1 Baiting Threat

Attacker in this type of social engineering collects information about victim interests, then uses this information to lure victims into a trap lead to steal their sensitive information or threat their computers. Biting attack depends on arousing the curiosity and greed of the victims [16]. For example, if a victim is interested in movies, the attacker can uses offer free downloading to trick the victim to disclose his/her information. Another example, an attacker can send a gift that contains a flash memory with malicious malware to pique victim's curiosity to open it and launch the attack.



SOCIAL ENGINEERING THREATS

3.2 Reverse Social Engineering Threat

In reverse social engineering, a victim unwittingly goes to the attacker after the attacker makes a problem for the victim and offers its help. The attacker aims to gain a trust of the victim then exploit this trust [16], [17]. The victim here establishes a trusted relationship with the attacker, while the attacker waits for this communication. For example, the attacker can disguise itself as a technical support person and send a fabricated email to the target, that email include the phone number of the attacker with text instruct the receiver of the message to asking for help if he/she need it. When the victim falls into the problem that making by the attacker, he\she will be asking the attacker for help [18]. Four types of reverse social engineering: direct, mediated, targeted and untargeted. In direct type, the baiting action is visible to the victim. While in meditated type, there is an intermediary which collects and propagates the baiting. The bad guys in the targeted type of reverse social engineering are targeting a specific user. While they aim to reach to a large number of people in untargeted type [18].

3.3 Pretexting Threat

Attacker here impersonating and creates a pretext to gain to the victim then steal its information. The most popular example of pretexting when the criminal's person pretends to call from the bank and need to confirm the victim identity [16], [19].

3.4 Watering Hole Threat

It is more advanced than other social engineering attacks because it requires good skills [18]. The attacker in watering hole targets victim that belongs to a group and monitors the activities of this group over the internet, then infects the website or an application which is visited by malware [16]. After that, the attacker tries to obtain only the victim information [20]. It is hard to detect [19].

3.5 Quid Pro Quo Threat

It is like pretexting attack which the criminal's person creates a reason to communicate with a target to exchange data with her\his. The main difference between them that the quid pro quo attack targets a specific person. In the bank example, the attacker masks itself as an employee in the bank tries to help the victims and asking them about sensitive information or asking for turn off the antivirus software in their computers. It is a successful attack in most cases [20], [21].

3.6 Phishing Threat

It is an art that aims to steal critical information like medical data, payment card details or addresses, or to get a benefit like getting money. The phisher disguising itself as a trusted entity to gain the victims' trust then exploit them. The phisher usually targets groups of people and contact with them over many channels like email, social media, phone calls and text messages [16]. There are many reasons of why people can be exploited easily, like a lack of computer security knowledge, visual deception tricks used by attackers and lack of interest in indicators of security [22]. Spear-phishing is a type of phishing when the attacker targets a specific victim. Because this type of phishing used advanced methods, it has a success rate higher than the traditional phishing [16].

3.7 Dumpster diving Threat

Attacker gathers information before the attack from victims' waste. The trash may contain a valuable data to the attacker [16]. The attacker search in trash about small information, like username, password, day planner, emails, phone numbers, operation manuals or IP addresses. The dumpster diving name coming from the meaning of dumping in undesirable garbage.

3.8 Shoulder Surfing Threat

Attacker gathers sensitive information about the target by looking over the target's shoulder. An attacker can implement this attack directly or using devices like camera or binoculars [16], [23].

3.9 Eavesdropping Threat
Attacker gathers information about the victims by secretly listening to them without their consent directly or using devices [16], [1].

3.10 Tailgating Threat
Type of threat when an attacker aims to unauthorized access to a restricted location. The most popular example of this type is when an attacker follows a legitimate person to enter a target location [16] [24]. Another example, when the attacker asks a computer from someone to download a malware [15].

4 COUNTERMEASUERS
It can be obvious that even though the security in networks is improved, people constantly remain the weakest part in the security system. The percentage of successful cyber-attacks are remained increasing because of the obscurity degree which social engineering provides to harmful software performers. Industries must always be aware of the countless attacks performers and their plenty numbers of threats or breaches in order to be capable of reply against it. There are technological and non-technological safety measure which could be applied to diminish the danger related to social engineering to an acceptable degree. Establishments add various levels to their security arrangements therefore if the method in the external level dose not succeed, a method in as a minimum single internal level could thwart a risk before becoming a catastrophe. This idea is identified as multi-level defenses or else a defense in depth. An excellence Protection in Depth erection contains a combination of the next preventive countermeasures [12]:

4.1 Security Policies
An efficient security policy should be accurately written, easy to reach, and based on morals and strategies of the proper security policy. In addition, it must be plainly written in understandable language for common people and apply it to each field in its range. Besides in every strategy, must specify morals and rules to follow in complying the strategy[1], [12] .

4.2 Education and training
This evolving employees' security consciousness by providing a training program where initially trained in the first days on the job and repeated additional training to refresh through the years. This will build the employees' awareness to thwart this kind of attacks [12], [25].

4.3 Inspections and Obedience
Establishments must dynamically authenticate that their security strategy is followed. Roughly investigator checks contain studying network logs, re-authenticating workers' authorizations, and inspection desktop activities at minimum twice per month [12].

4.4 Authentication and Permission Measures
Doubt is Good! No info without authentication! Never afford a little special or private info throw phones, texts, or internet to anybody except when you could authenticate who he is and make sure that human has a real requirement for this info [14]. Teach employees that they should authenticate the identification of the individual who request some data or activity to be done and guarantee that the individual is allowed to take this demanded data or to give an instruction to do an activity [26].

4.5 Shredded and Burning
Workers are repeatedly tricked to reveal a confidential info through social engineers who masquerade as an information technology specialist from the establishment. Rid-of slightly confidential papers by shredding it, protect employee's computer by anti-virus software and most of all remember that doubt is healthful [8].

4.6 Checked your State
There are many security organizations that businesses and people deal with to help and guard opposite to the danger of social engineering. These organizations measure your network or company weaknesses to social engineering outbreak [14].

4.7 Anti-phish
'Phishing attack' is the most famous technique of social engineering. E-mails that person is getting where it requests a confidential info by pretending to be as trustful established. There is also similar way some Emails readdress users to forge electronical sites that is a like for a trustful one to get their private data this way is called 'Pharming'. To thwart these threats, there are a quite a lot of security software that fight back against these attacks. However, employee's awareness is playing a big role also in avoiding these attacks because there is no replacement for their alertness and awareness [14].

4.8 Using Accurate Software
Firewalls and anti-virus software are extremely vital for every network used for clear details. However, recently there are a famous traffic filtering system and software, which rise the internet security throw stopping a harmful website and thwart the danger of becoming a victim to this kind of attacks. Furthermore, users must keep their system updated because this will help to repair security vulnerabilities in the system [14].

5 DISCUSSION

Table I: *Attacks and countermeasure*

Countermeasure	Attack
Security Policies	Tailgating
Education and training	▪ Baiting ▪ Reverse Social Engineering Threat ▪ Eavesdropping ▪ Shoulder Surfing ▪ Pretexting ▪ Quid Pro Quo
Anti-phish	Phishing
Shredded and Burning	Dumpster diving
Authentication and permission measures	Tailgating
Using accurate software	Watering Hole

As mentioned in the previous section that there are no grantee countermeasures that will thwart the social engineering attacks, but there are some main countermeasures if individuals or companies follow it will help to prevent from this kind of attacks. It can be seen summarized in the table 1 based on our study we discover that education is one of the most effective methods for avoiding social engineering attacks because when increasing the person's awareness, it becomes difficult to attacker to trick them by any means. Furthermore, using policies to give the least privileges to each employee is a sufficient way to ensure that no one can access the data unless they authorized to after using authentication methods. In addition, destroying any papers or multimedia that contain sensitive data is one of the effective ways to avoid dumpster diving attack. Indeed, using some anti-viruses' software can be a huge help to thwart the danger that coming from the watering hole attack.

6 CONCLUSION

In our survey paper we discussed various topics of social engineering and their common techniques and we mentioned some details about the motivations that trigger attackers to perform such malicious acts, and why people fall for them which mainly addressed under the lack of technological knowledge and expertise, and we argued some proposed countermeasures against social engineering attacks. We hope by finishing this paper to help presenting a good understanding of social engineering from all perspectives as possible, and since this type of attacks still don't have many "tools" to detect it and prevent it. Despite the fact that social engineering is a non-technical way of exploiting human weaknesses, we hope in the future that there will be a tool which can help to discover this kind of attack faster and accurately to thwart it.

REFERENCES

[1]. R. Gulati, "The threat of social engineering and your defense against it," SANS Reading Room, 2003.

[2]. A. Koyun and E. Al Janabi, "Social engineering attacks," Journal of Multidisciplinary Engineering Science and Technology (JMEST).

[3]. K. Zetter, "Google hack attack was ultra sophisticated," New Details Show.

[4]. I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh, "Social engineering attack strategies and defence approaches," in 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), pp. 145-149.

[5]. D. I. van Liempd, A. Sjouw, M. Smakman, and K. Smit, "Social Engineering As An Approach For Probing Organizations To Improve It Security: A Case Study At A Large International Firm In The Transport Industry."

[6]. A. Chitrey, D. Singh, and V. Singh, "A comprehensive study of social engineering based attacks in india to develop a conceptual model," International Journal of Information and Network Security, vol. 1, p. 45.

[7]. N. Y. Conteh and P. J. Schmick, "Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks," International Journal of Advanced Computer Research, vol. 6, p. 31.

[8]. J. K. Burgoon and T. R. Levine, "Advances in deception detection," New directions in interpersonal communication research, vol. 20.

[9]. A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," Science, vol. 347, pp. 509-514.

[10]. S. Abraham and I. Chengalur-Smith, "An overview of social engineering malware: Trends, tactics, and implications," Technology in Society, vol. 32, pp. 183-196.

[11]. M. Junger, L. Montoya, and F.-J. Overink, "Priming and warnings are not effective to prevent social engineering attacks," Computers in human behavior, vol. 66, pp. 75-87.

[12]. N. Y. Conteh and P. J. Schmick, "Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks," International Journal of Advanced Computer Research, vol. 6, p. 31, 2016.

[13]. I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh, "Social engineering attack strategies and defence approaches," in 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), 2016, pp. 145-149.

[14]. A. Adewole, A. Durosinmi, and M. A. Polyetchnic, "Social engineering threats and applicable countermeasures," African Journal of Computing & ICT, vol. 8, 2015.

[15]. F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," Future Internet, vol. 11, p. 89, 2019.

[16]. P. P. Parthy and G. Rajendran, "Identification and prevention of social engineering attacks on an enterprise," in 2019 International Carnahan Conference on Security Technology (ICCST), 2019, pp. 1-5.

[17]. D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda, and C.

Pu, "Reverse social engineering attacks in online social networks," in International conference on detection of intrusions and malware, and vulnerability assessment, 2011, pp. 55-74.

[18]. A. Koyun and E. Al Janabi, "Social engineering attacks," Journal of Multidisciplinary Engineering Science and Technology (JMEST), 2017.

[19]. C. Hadnagy, Social engineering: The art of human hacking: John Wiley & Sons, 2010.

[20]. S. Lohani, "Social Engineering: Hacking into Humans," International Journal of Advanced Studies of Scientific Research, vol. 4, 2019.

[21]. D. van Liempd, A. Sjouw, M. Smakman, and K. Smit, "Social Engineering As An Approach For Probing Organizations To Improve It Security: A Case Study At A Large International Firm In The Transport Industry," 2019.

[22]. R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in Proceedings of the SIGCHI conference on Human Factors in computing systems, 2006, pp. 581-590.

[23]. X. Luo, R. Brody, A. Seazzu, and S. Burd, "Social engineering: The neglected human factor for information security management," Information Resources Management Journal (IRMJ), vol. 24, pp. 1-8, 2011.

[24]. K. Ivaturi and L. Janczewski, "A taxonomy for social engineering attacks," in International Conference on Information Resources Management, 2011, pp. 1-12.

[25]. A. Algarni, Y. Xu, T. Chan, and Y.-C. Tian, "Social engineering in social networking sites: Affect-based model," in 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), 2013, pp. 508-515.

[26]. W. R. Flores and M. Ekstedt, "Countermeasures for Social Engineering-based Malware Installation Attacks," in CONF-IRM, 2013, p. 23.