CHAPTER-11

Social engineering and Vulnerability with Human Mind

Farhan Beg[1], Sowmya K.N[1], H.R Chennamma[2]

[1,2] *Department of Information Science and Engineering, JSS Academy of Technical Education, Bangalore, India*

[3]*Department of Computer Applications, JSS Science and Technology University, Mysuru,* anuamruthesh@gmail.com

***Corresponding Authors**

Email: *kn_sowmya@rediffmail.com, farhanbeg@jssateb.ac.in*

Abstract

Social engineering is a method to psychologically manipulate someone by giving out personal details about them[1]. A perpetrator first investigates and evaluates the victim before engaging in social engineering. The attacker makes further efforts to perform actions that interfere with their security after gaining the victim's confidence and trust. Once the victim believes the attacker, they gain access to private and crucial information. According to the FBI's 2019 Internet Crime Report, criminals only used corporate email breaches to steal more than $1.7 billion[2][3]. Social engineering scams typically cost $130,000 [4] in lost revenue or lost data. Hackers apply the six manipulative social tactics -Reciprocity, Commitment, Social Proof, Authority, Liking, and Scarcity[5]. Discovery & Investigation, Deception & Hook, Attack and Retreat are the four phases of social engineering[6]. Hackers learn more about their target's phone number, email address, and social media to get in touch with you. Small cybersecurity mistakes cost a lot to companies or businesses. A company data breach typically costs about $3.86 million[7]. It might take up to 200 days to become aware of a cyberattack or data breach until it's too late[8]. There are different types of social engineering attacks, the 8 most common types of social engineering attacks are baiting, catfishing, pretexting, phishing, scareware, tailgating & piggybacking, water holing, and quid pro quo[9]. Phishing comes in the forms of spear phishing, vishing, and phishing emails whose main motive is to extract sensitive content and information of the user[10]. Social engineering is one of the largest cybersecurity dangers facing both small and large enterprises. Social engineering causes financial losses, Business Disruption, and Damage To Reputation. Using multi factor authentication, and teaching employees how to spot phishing scams will avoid falling victim to social engineering. Restrict access to your systems to just authorized devices. Also, any email sent from an external source should have a warning banner, such as "external email," attached. These steps could help in staying safe from social engineering attacks.

Keywords: Social Engineering, Phishing Attacks, Cyber Attacks

Introduction

The usage of social engineering is increasing in recent years in many good and bad ways. According to the Oxford English Dictionary, the term "social engineering" has two separate meanings[11]. First, it is "the use of centralized planning in an attempt to manage social change and regulate the future growth and behavior of a society", Second, it is “the use of deception to persuade someone to expose private information or, more specifically, to unintentionally grant unauthorized access to a computer system or network”. Both definitions involve one or more people influencing others behavior, but the former expressly has applications in the fields of political and economic management, whilst the latter has a special place in the world of the internet.

Social engineering is a method to psychologically manipulate someone by giving out personal details about them or doing something beneficial for the attacker[12]. A perpetrator initially looks into and assesses the victim in social engineering. In this process, the victim's fundamental background information is obtained, which may include security mechanisms and access points that could be vulnerable to assault. After winning the victim's trust, the attacker attempts to carry out additional operations that interfere with their security procedures. Once the victim starts to trust the attacker, they might have access to sensitive data or vital, secure resources. It helps the attacker to get crucial access to begin the attack or at a later stage allows the attacker to get out of a situation he is stuck in or to continue the attack to its destiny, there are many crucial points in an attack when social engineering is the only option left to the attacker[13]. Social engineering is based on human decision making known as cognitive biases[14]. These biases are sometimes referred to as a bug in the working of the human mind, these bugs are exploited in various social engineering techniques. Knowing how to take advantage of these biases is one of the basic skills required to perform a successful social engineering attack on the target. Social engineering attacks are one of the most dangerous threats in the world, according to the US Department of Justice[15]. Over 700 social engineering attacks are directed against the typical organization each year[16]. Cybercriminals and hackers from all over the world specifically target and have a big impact on U.S. corporations. When these organizations are hacked, it significantly impacts both privacy and the global economy because they manage precious, multinational data. In the US, these attacks are estimated to have cost US $121.22 billion[17]. In this work we aim to make people aware of the process of social engineering., the importance of social engineering, and the impacts of social engineering.

Key Principles of Social Engineering

Notorious cybercriminals who break into computers. By relying on societal norms, ignorance, and the good faith of their victims, social engineers manipulate people's minds. Hackers use the six principles of social influence, which marketing and psychology professor Robert Cialdini listed in 1984[18]. These ideas influence how people relate to one another and have the potential to be persuasive. Social engineering relies heavily on six key principles[19] which can be considered as six pillars of social engineering [20]. These six principles are depicted in Figure 1:

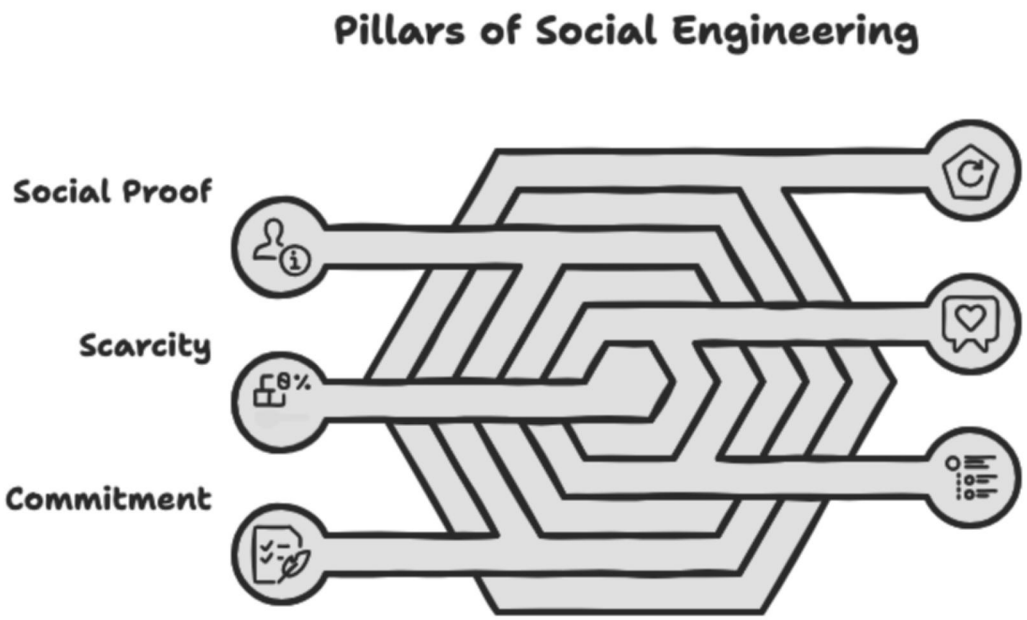

Figure 1: Key Principles of Social Engineering

1) **Reciprocity:** People typically desire to give back to those who have helped them, whether it favors our, knowledge, or a tangible item. Hackers take advantage of this by delivering their targets tiny presents or "useful" information on goods and offset to win their trust[21].

2) **Commitment:** Written agreements or agreements to which people have given their approval are usually honored. Hackers have been known to deceive victims into believing they have signed up for a service or subscription to force them into providing payment and login information[22].

3) **Social Proof:** Monkeys learn through doing. People will imitate what they see other people doing, whether it's using the same product as a reliable source or getting in line with everyone else even though there isn't a sign directing them to. These lines, such as "Debbie over in accounting sent me her passwords — I'll need yours, too," are being used by hackers[23].

4) **Authority:** Less discretion will be exercised in obeying superiors' superiors' directions than peers. Because of this, hackers frequently pretend to be managers or supervisors to get access. It's also the reason why getting into places while dressed as an authority figure, such as an electrician or construction worker, frequently goes unnoticed[24].

5) **Liking:** Someone often obeys directions from people they like, which is similar to deferring to authority. Hackers use this to their advantage by impersonating friends or family members or building trust with their victim before an attack.

6) **Scarcity:** Something becomes more desirable or urgent if it is scarce or limited. This is why timers are frequently affixed to ransomware campaigns and phishing emails, confusing the targets and causing them to freak out.

Process of Social Engineering

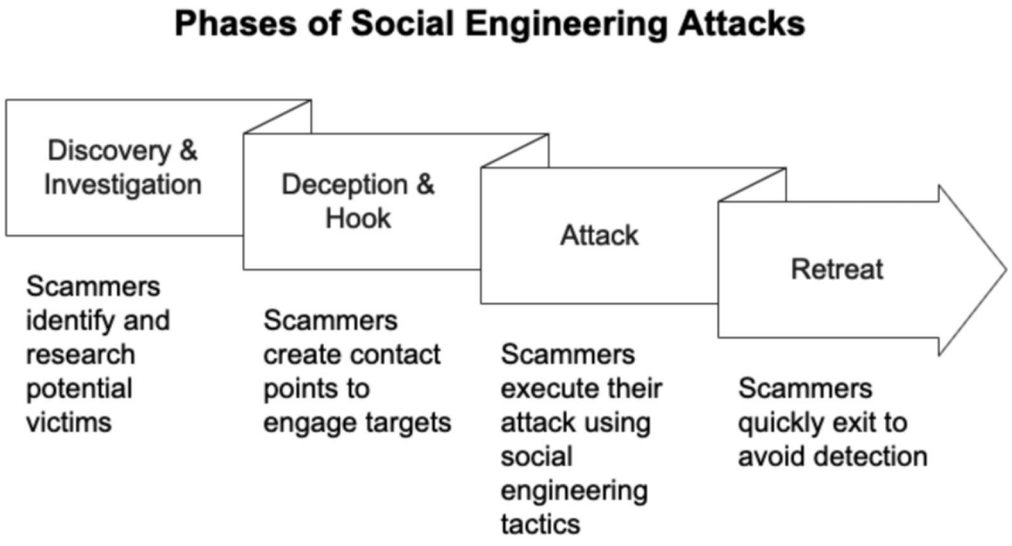

Figure. 2: Process of social engineering

Attacks through social engineering are comparatively simple. A hacker only needs to persuade one uninformed, overworked or trusted individual to act as instructed. The outcomes are worthwhile as well. Hackers deceived Twitter employees into giving them access to internal tools in one of the most well-known social engineering assaults of all time. The hackers then attempted to trick their large following into sending Bitcoin to them by compromising the accounts of celebrities like Joe Biden, Elon Musk, and Kanye West. These assaults all have a similar structure and are relatively simple to execute. The four phases [19] of social engineering are depicted in figure 2 and are as follows.

1) **Discovery & Investigation:** Scammers begin by choosing people who possess the desired item. Credentials, data, unlawful access, money, private information, etc. are typical examples. Then they search online for possible victims. They might check your online footprint, examine where you work, notice what you post on social media, and other things, for instance. Once they have your identity, the hackers utilize it to create the ideal, specialized assault. Additionally, you'll be more likely to let your guard down given how much the assailant knows about you[19].

2) **Deception & Hook:** Scammers will search for prospective entrance points as they gain more information about their targets. They may be your email address, phone number, or social media account - anything that would allow them to contact you and allow them to launch an assault. Once they have your interest, they will then make contact with you. Consider the scenario where you have received a new work title and announced it on LinkedIn. A scammer could easily pose as an email from a reputable business website and invite you to an interview. Why wouldn't you answer if it seemed innocent and commonplace?[25]

3) **Attack:** When the hook draws you in, the scammer uses one of the numerous social engineering strategies to get you. For instance, the scammer discreetly installs malware on your device after you click the link to schedule an online interview. The next thing you know, your entire company's network is infiltrated, and gigabytes of private information has been taken by the con artist. Small cybersecurity errors like this can cost businesses a lot of money. A firm data breach often costs a whopping $3.86 million[26].

4) **Retreat:** Once criminals have completed their tasks, they will disappear as quickly as possible. You won't even be aware of what happened until it's too late because it takes up to 200 days on average to notice a cyberattack or data breach[27].

Types of Social Engineering

The 8 most common types of social engineering attacks[3] that are being used nowadays to target the victim depend on his weakness or can be said as vulnerabilities in his brain and are depicted in Figure 3.

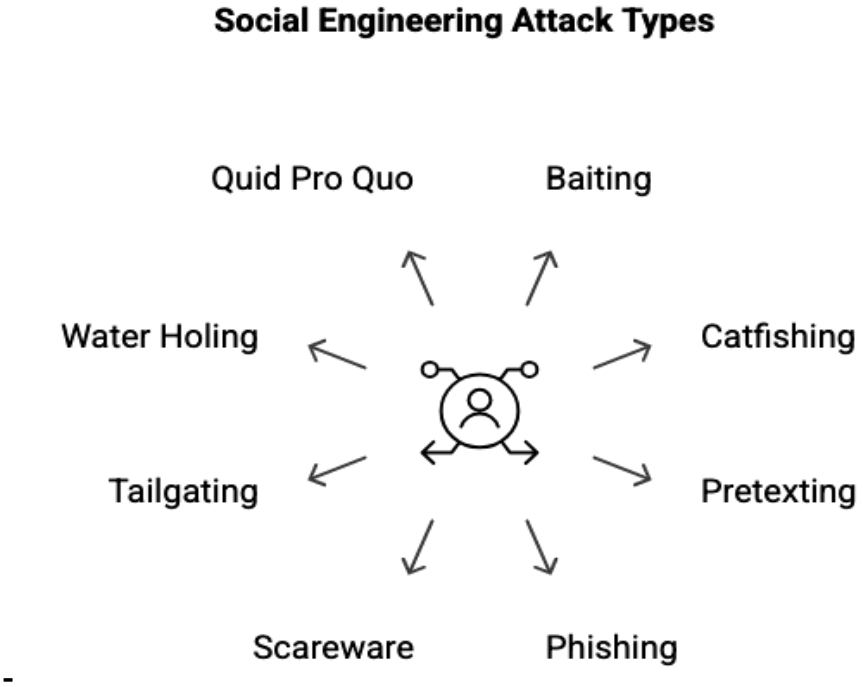

Figure 3: Common social engineering attacks

1) **Baiting:** As the term implies, baiting preys on the curiosity or greed of a victim. The attacker sets up a trap to pressure the victim into doing a particular action. A USB drive left on a desk unattended is an illustration of physical bait. It would prompt the intended victim to plug it in to see what's inside. Unknown to the victim, it can be installing malicious software like ransomware on the victim's computer. However, baiting can also be done online. In online mode, it can be done with an appealing commercial or an online form [28][29][30].

2) **Catfishing:** Catfishing is a well-known example of social engineering. It is a dishonest practice centered on forging a false identity to gain a victim's trust. Romance fraud, whose prevalence has risen sharply in recent years, is closely related. A honey trap is a real-life version, in which the assailant poses as being romantically interested in the victim to get what they want[31][32][33].

3) **Pretexting:** Attackers can persuade victims that they are a coworker, bank officials, or representatives of the government by weaving several lies together. They establish relationships with the individual and convince them to respond to security queries to verify their own identity. The psychological ploy puts victims on the defensive, making them feel as though they must clear their names, which leads them to divulge crucial personal information (such as their social security number, bank account information, etc.)[34][35].

4) **Phishing:** Phishing is the most common type of social engineering attack performed. Phishing and other similar attacks like vishing etc. are all the same but have some technical differences[36].

Figure. 4: Understanding phishing attacks

The main goal of all methods is to get sensitive data out of the target.

- **Phishing:** Any communications campaign intended to send the target to a certain form, website, or checkout. Examples of common scams include text messages that lure victims to a fake bank website by instructing them to log into their accounts. In 2020, phishing was the most frequently reported issue by both individuals and corporations, costing them $1.8 billion in lost revenue[37].
- **Vishing:** Phishing is the same as phishing just different execution, it is carried out via audio technology, like a Skype call or false voicemail[37].
- **Spear-Phishing:** Targeted phishing that focuses on a specific person is known as spear phishing. Due to their access to critical firm information, business executives or customer service workers are increasingly being targeted[38].
- **QRishing:** Phishing scams using Quick Response Codes(QR Codes), in this person is scammed using fake QR codes or attacker-controlled QR codes. As QR codes are being used everywhere nowadays, it is quite easy to make a victim scan an attacker-controlled QR code, even if the victim finds something suspicious he will most probably still scan it just out of curiosity which accomplishes the goal of the attacker[39].
- **Smishing:** It is a type of phishing in which the victim is targeted through an SMS service[40].
- **Angler Phishing:** A recent variation of phishing attacks that target users of social media is called angler phishing. On social media, people pose as customer support representatives to contact irate customers and request their personal information or login credentials [41].

It's important to note that deep fake phishing has become more prevalent recently, both for voice and video[42]. By feeding video footage of actual people to software and retraining it to say whatever they want, fraudsters may now impersonate someone. It is frequently used in the context of social engineering to establish trust, such as when asking a worker to wire money to a certain account while pretending to be an executive.

5) **Scareware:** Because scams are most effective when the target is stressed out, hackers have developed a whole class of software they call scareware. It involves intimidating the victim into taking an action, such as downloading a harmful antivirus under the guise of resolving a computer issue. Scareware frequently targets older, less tech-savvy generations and is disseminated by spam emails or pop-up ads[43][44].

6) **Tailgating & Piggybacking:** The iconic heist film, in which bad guys pose as a janitor or delivery persons to enter off-limits regions. Even though most corporate settings have security measures in place to prevent this kind of intrusion, if you're sufficiently confident, it can be surprisingly simple to sneak past a front desk[45][46].

7) **Water Holing:** Regular website visitors have already developed a relationship of trust with the business. A victim might not click a link from an unfamiliar email account, but if the link is on a website they frequently visit, they won't have any trouble clicking it. In a water hole attack, malicious code is directly injected into a website that the victim is known to frequently visit[47][48].

8) **Quid Pro Quo Attack:** Attacks known as quid pro quo are so termed after the Latin phrase for a favor given in exchange for something. Simple promises of services or goods in exchange for the fraudsters' desired items are all that these attacks involve. The funny thing is, the bar doesn't need to be very high. Employees have been targeted successfully for attacks just by promising them a bar of chocolate in exchange for their login information[49][50].

Impact of Social Engineering

Every year, social engineering or spear phishing attacks target more than 50% of all businesses? The number is alarming, and social engineering is currently one of the largest cybersecurity dangers facing both small and large enterprises. However, for a variety of reasons, many business owners choose not to invest in their organization's cybersecurity. Consider these five effects of social engineering attacks to assist you to decide if you're still on the fence about employing a cybersecurity firm to advise your company:

1. **Financial Losses:** The only impact of cyber security incidents that everyone is aware of is the amount of money the company suffers as a direct consequence of a social engineering attack. Depending on the size of your company and the attacker's avarice, this amount could vary from around $20,000 to millions of dollars[51].

2. **Loss of Productivity:** Any successful cyberattack drastically disrupts regular business activities. Whereas the IT team and many management-level employees put off their other jobs to deal with the breach, all staff members must be told about it and instructed on how to prevent a similar attack in the future, among other things. All of this interferes with the employee's commitments at work and significantly lowers productivity[13].

3. **Cost of Recovery:** The recovery cost, which includes the money required to hire an incident response team, buy software that will stop a similar assault from happening in the future, and deal with clients whose data was stolen during the attack, is another typical expense linked to spear-phishing attacks[13].

4. **Business Disruption:** Similar to productivity loss, this social engineering effect also evaluates how the hack impacts your supply chain and consumer satisfaction ratings. If a hacking attempt is successful and disrupts your normal business activities, your organization may experience delays in the production of products, shipping, or other operations. As a result of this, you can lose clients or even suppliers. Additionally, your bank and insurance

provider could wish to review your company's cybersecurity protocols following the incident[52].

5. **Damage To Reputation:** If a company suffered a significant cybersecurity problem while you were a customer or a supplier, how likely are you to trust it again? Would you continue doing business with this company? Because people are reluctant to put themselves or their information at risk, many businesses experience significant customer and supplier losses following a security breach. Unfortunately, many firms are like this[53].

Staying Safe from Social Engineering

Awareness of how a social engineering attack progresses, what impact it has, and what weaknesses it targets, we can adopt a conscious way to be safe from social engineering and few approaches have been discussed here.

- ***Secure Most Valuable Assets From Attack:*** Focus on and save the most valuable assets in an attack for example financial assets personal documents etc by restricting access to save from attackers which can cause a huge loss to the owners.
- ***Conducting Phishing Awareness Training and Testing:*** Make sure that employees are on the lookout for emails that are phishing attempts and that they have time to reflect on the tests afterward to recognize these attacks more quickly and learn when not to click. According to our research, this works best in small groups where participants discuss how to recognize phishing scams and share their personal social engineering experiences. Instilling this kind of culture in business is essential.
- ***Using Multi Factor Authentication:*** Multifactor authentication is a fantastic deterrent against straightforward password theft, even though it was broken in the current Twitter hack. Almost all significant cloud systems support multi factor authentication, and if they don't, it might be time to think twice before utilizing them.
- ***Use of Corporate Machines To Access Systems:*** Many businesses let users log into their corporate networks from any device. You may greatly enhance your security posture by establishing a policy that forbids doing this. It's just not a good idea to provide staff access to your system on a device that you don't control, where they can install anything they want and where their adolescent children might use it.
- ***Enforce That Only Authorized Machines Can Access Systems:*** Ensure only authorized machines access systems, implement device authentication using digital certificates and protocols like 802.1X. Employ endpoint management tools, enforce access control policies (e.g., Zero Trust, RBAC), and secure communication via encryption and VPNs. Regular monitoring, geofencing, and compliance with industry standards further enhance security, while tools like MDM and SIEM streamline enforcement and detection.

- ***Must Have An Incident Response Plan:*** Before something horrible occurs, it's crucial to have a strategy in place so that you know what to do and how to contact your stakeholders. Effective post-breach communication has been difficult for several firms, which has negatively affected those businesses.
- ***Use Advanced Tools:*** Use anti-phishing, sandboxing, and URL rewriting technologies to ensure that all files are opened before they reach your email account and that no one can access an email-sent site without it first being confirmed by a provider. Microsoft, Mimecast, and Proofpoint all offer excellent tools.
- ***Be Alert: Never Trust, and Always Check:*** Common sense can beat any cyber attack by being vigilant. Be on the lookout for clues that someone isn't who they say they are or doesn't know you. Before wiring $50,000 to an arbitrary account, call your manager to seek their approval. If money is involved, you should confirm any contacts that don't seem right. Another word of advice from the FBI: "Be extremely skeptical if the requester is urging you to comply immediately."

Conclusion

In this work, a brief review of key principles of social engineering, types of social engineering, the process of social engineering, impacts of social engineering, and at last how to be safe from social engineering is discussed. We cannot consider ourselves safe if just our systems are safe but we need to be alert and at times suspicious of everything happening around us in the virtual world related to the physical world to be safe and yet no one can guarantee your safety. In our opinion, "A human mind is full of vulnerabilities. It depends on the owner of that brain at that instant of time to determine the vulnerabilities that have been left to be exploited".

References

1. Hinson, M. (2008). Social engineering techniques, risks, and controls. The EDP Audit, Control, and Security Newsletter archive 37: 32-46.
2. Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., ... & Bursztein, E. (2017, October). Data breaches, phishing, or malware? Understanding the risks of stolen credentials. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security* (pp. 1421-1434).
3. Garfinkel, S. (2002). The FBI's cybercrime crackdown. *TECHNOLOGY REVIEW-MANCHESTER NH-*, *105*(9), 66-75.
4. Alsulami, M. H., Alharbi, F. D., Almutairi, H. M., Almutairi, B. S., Alotaibi, M. M., Alanzi, M. E., ... & Alharthi, S. S. (2021). Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia. *Information*, *12*(5), 208.

5. Ferreira, A., Coventry, L., & Lenzini, G. (2015, August). Principles of persuasion in social engineering and their use in phishing. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 36-47). Springer, Cham.

6. Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014, August). Social engineering attack framework. In *2014 Information Security for South Africa* (pp. 1-9). IEEE.

7. Alexei, L. A., & Alexei, A. (2021). Cyber security threat analysis in higher education institutions as a result of distance learning. International Journal of Scientific and Technology Research, (3), 128-133.

8. Tweneboah-Kodua, S., Atsu, F., & Buchanan, W. (2018). Impact of cyberattacks on stock performance: a comparative study. Information & Computer Security.

9. Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of Social Engineering Attacks on Social Networks. Procedia Computer Science, 198, 656-661.

10. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. Cryptography, 2(1), 1.

11. Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. Computers & Security, 73, 102-113.

12. Heartfield, R., & Loukas, G. (2015). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. _ACM Computing Surveys (CSUR)_, _48_(3), 1-39.).

13. Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 89.

14. Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social engineering: The neglected human factor for information security management. _Information Resources Management Journal (IRMJ)_, _24_(3), 1-8.

15. Social engineering (security). (2022, October 15). In *Wikipedia*. https://en.wikipedia.org/wiki/Social_engineering_(security).

16. Turner, J., & Wagstaff, L. Investigating the use of social media for Social Engineering Attacks.

17. AL-Otaibi, A. F., & Alsuwat, E. S. (2020). A study on social engineering attacks: phishing attack. _International Journal of Recent Advances in Multidisciplinary Research_, _7_(11), 6374-6380.

18. Cialdini, R. B., & Griskevicius, V. (2010). Social influence.

19. Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, *59*, 186-209.

20. Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. _Annual review of psychology_, _55_(1), 591-621.

21. Uebelacker, S., & Quiel, S. (2014, July). The social engineering personality framework. In _2014 Workshop on Socio-Technical Aspects in Security and Trust_ (pp. 24-30). IEEE.

22. Lord, A. T., & DeZoort, F. T. (2001). The impact of commitment and moral reasoning on auditors' responses to social influence pressure. _Accounting, organizations and society_, _26_(3), 215-235.

23. MacCoun, R. J. (2012). The burden of social proof: Shared thresholds and social influence. _Psychological review_, _119_(2), 345.

24. Milgram, S., & Gudehus, C. (1978). Obedience to authority.

25. Indrajit, R. E. (2017). Social engineering framework: Understanding the deception approach to human element of security. _International Journal of Computer Science Issues (IJCSI)_, _14_(2), 8.

26. Ghazi-Tehrani, A. K., & Pontell, H. N. (2021). Phishing evolves: Analyzing the enduring cybercrime. _Victims & Offenders_, _16_(3), 316-342.

27. Ayyagari, R. (2020). Data breaches and carding. In _The Palgrave Handbook of International Cybercrime and Cyberdeviance_ (pp. 939-959). Palgrave Macmillan, Cham.

28. Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of Social Engineering Attacks on Social Networks. *Procedia Computer Science*, *198*, 656-661.

29. Saleem, J., Adebisi, B., Ande, R., & Hammoudeh, M. (2017, July). A state of the art survey-Impact of cyber attacks on SME's. In _Proceedings of the International Conference on Future Networks and Distributed Systems_.

30. Koyun, A., & Al Janabi, E. (2017). Social engineering attacks. _Journal of Multidisciplinary Engineering Science and Technology (JMEST)_, _4_(6), 7533-7538.

31. Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547-559.

32. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2013, November). Social engineering attacks on the knowledge worker. In _Proceedings of the 6th International Conference on Security of Information and Networks_ (pp. 28-35).

33. Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. _Computers in Human Behavior_, _75_, 547-559.

34. Hadnagy, C. (2010). *Social engineering: The art of human hacking*. John Wiley & Sons.

35. Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American society for information science and technology*, *59*(4), 662-674.

36. Ferreira, A., Coventry, L., & Lenzini, G. (2015, August). Principles of persuasion in social engineering and their use in phishing. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 36-47). Springer, Cham.

37. Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4), 297-307.

38. Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016). Breaching the human firewall: Social engineering in phishing and spear-phishing emails. *arXiv preprint arXiv:1606.00887*

39. Vidas, T., Owusu, E., Wang, S., Zeng, C., Cranor, L. F., & Christin, N. (2013, April). QRishing: The susceptibility of smartphone users to QR code phishing attacks. In *International Conference on Financial Cryptography and Data Security* (pp. 52-69). Springer, Berlin, Heidelberg.

40. Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4), 297-307.

41. O'Hagan, L. (2018, June). Angler phishing: Criminality in social media. In *5th European Conference on Social Media ECSM* (p. 190).

42. Simmons, M., & Lee, J. S. (2020, July). Catfishing: A look into online dating and impersonation. In _International Conference on Human-Computer Interaction_ (pp. 349-358). Springer, Cham.

43. Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. (2022). Social Engineering Attacks Prevention: A Systematic Literature Review. *IEEE Access*.

44. Heartfield, R., & Loukas, G. (2015). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. _ACM Computing Surveys (CSUR)_, _48_(3), 1-39.

45. Seifert, C., Stokes, J. W., Colcernian, C., Platt, J. C., & Lu, L. (2013, May). Robust scareware image detection. In *2013 IEEE International Conference on Acoustics, Speech and Signal Processing* (pp. 2920-2924). IEEE.

46. Breda, F., Barbosa, H., & Morais, T. (2017, March). Social engineering and cyber security. In *International Technology, Education and Development Conference* (Vol. 3, No. 3, pp. 106-108).

47. Costa, L. Social Engineering Attacks: Risks, Vulnerabilities and.

48. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2013, November). Social engineering attacks on the knowledge worker. In _Proceedings of the 6th International Conference on Security of Information and Networks_ (pp. 28-35).

49. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2013, November). Social engineering attacks on the knowledge worker. In *Proceedings of the 6th International Conference on Security of Information and Networks* (pp. 28-35).

50. Ivaturi, K., & Janczewski, L. (2011). A taxonomy for social engineering attacks.

51. Breda, F., Barbosa, H., & Morais, T. (2017, March). Social engineering and cyber security. In *International Technology, Education and Development Conference* (Vol. 3, No. 3, pp. 106-108).

52. Hall, G. A. (2012). *Credit Card Fraud and Social Engineering: Mitigation of Identity Theft Related Losses Requires More Than Technology* (Doctoral dissertation, Utica College).

53. Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 31.

□□□