International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 14, Number 7 (2021), pp. 601-606

Spreading Awareness towards Social Engineering Attacks

Moaiad Ahmad Khder (Corresponding author)[1] , Latifa Khalid AlNoaimi[2]

[1,2] Department of Computer Science, Applied Science University
P.O. Box 5055, Building 166 | Road 23 | Block 623 | East Al-Ekir, Bahrain.

Abstract

Humans are the weakest link to hack any organization or any of their personal accounts. Social engineering with regards to information security is the art of human manipulation with performing attacks for disclosing confidential and serious information. Social engineering is a very serious threat in this generation due to the development of social engineering attacks. Despite the related methods have existed for quite a while, current awareness of social engineering and its numerous types is generally low, and endeavors are hence required to improve the security of the users. Although, some social engineering attacks have some characteristics and types in common, but it differs in the way the attack is performed. The purpose of this research is to show the social engineer's attacks characteristics, types, the theorem behind each one of the attacks and how to prevent it. The security of data is critical in a recent society and despite the fact that the security around data is ceaselessly improving, the one powerless point is as yet the person who is cannot control procedures. This research explained the attack vector and characteristics of social engineering in general term It is would be desirable that this research will familiarize the users with the attacks and will steer them to avoid it and protect themselves from being attacked.

Keywords: Social engineering, attacks, phishing, spear phishing, vishing, baiting, tailgating, pretexting, quid pro quo, hacking

1. INTRODUCTION

Recently the number of people losing control over their email or social networking account has increased to more than 15% of internet users proven by a research google conducted between March 2016 and March 2017 as there are 12.4 million victims of phishing kits only (Margolis, et al., 2017). There are various types of social engineering attacks and when information security fails to protect the system it is more likely because of human blunder not the system (Hartel, et al., 2018). Social engineering attacks are phishing, spear phishing, baiting, vishing, tailgating, pretexting, and quid quo pro.

2. RELATED STUDIES

2.1 Characteristics of social engineering attacks:

There are three characteristic of social engineering attacks as figure 1 is showing (Weippl, et al., 2013):

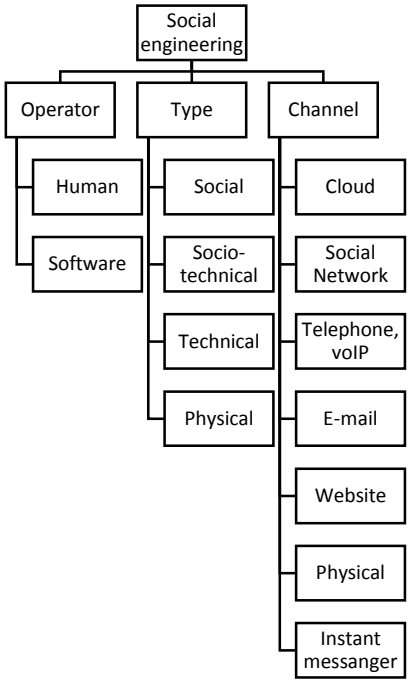

Fig. 1. Characteristics of Social Engineering attacks

The channel means where the attacker is performing the attack through it which could be cloud, social network, telephone, voice over IP, E-mail, website, physical, and instant messenger. However, the type of the attack could be social, combination of social engineering and technical Subterfuge, physical, and technical. Furthermore, the there are two types of operation which is the originator of social engineering attacks and it is includes human and software.

2.2 Social engineering type of attacks:

Phishing: The term phishing was first utilized in 1996 and it is considered to be cybercrime as it is a technique to deceive people to get their personal and financial information or send money directly to fund the attackers via sending emails as the attacker impersonate a trusted person or organization (Rittenhouse, et al.,2016). Nowadays, phishing is not only related to emails, but it is carried through multiple aspects in our life such as social networking sites, voice messaging, SMS,

instant messaging, and even multiplayer games (Hong, 2012).

The standard phishing attack contains three parts which are the lure, the hook, and the catch. The lure is most regularly an email message that has all the earmarks of being from a genuine organization, for example, a bank or network access supplier. The message contains a connection to the hook, and it is frequently covered up by muddling the URL while the hook is a site that impersonates the site of the real foundation which the victim or phish is eager to unveil private data to it. However, the catch includes the phisher utilizing the gathered data (Jakobsson & Myers, 2006).

Phishing is a combination of social engineering and technical Subterfuge. Social engineering alludes to tricking an individual to achieve certain objectives, which might be malevolent and harm people.

These methods essentially expect to get access to a certain system or getting data identified with an individual or multiple people for monetary benefit. Amid 2014, Apple was the most focused on brand by the phisher as indicated by worldwide phishing overview. Attacker sent phony messages to apple clients which requested that they update their account, giving a link to divert them to site where they could update the information, a few clients wound up giving their accreditation on those counterfeit sites. A phisher not simply depends just on the social engineering plans to robbery victim data. Technical subterfuge is another prominent method to extortion in which a phisher sends some pernicious code either joined with messages, or with sites, or with some self-executable code. (Gupta, Arachchilage, & Psannis, 2018).

Spear phishing: On the contrary of phishing emails which are generally and sent in mass to countless. spear phishing messages are sent and made for a specific individual or specific small category of individuals (McCormac, et al., 2016). Spear phishing is additionally being utilized against important targets, for example, corporate administrators or government authorities, in another name the attack is called "whaling" (Rittenhouse, et al.,2016). Another study showed that 72% of victims were attacked by their friends (Menczer, et al., 2007). Various of well know companies were targeted by the attackers for example RSA as the company suffered from an attack after the employee opened an attached in the e-mail, they found in the junk mail folder. Also, there is a research report showed the majority of spear phishing attacks against diplomatic, governmental, and research organization were located in former USSR Republics in Eastern Europe and Central Asia (Weippl, et al., 2015).

Baiting: Baiting is another social engineering technique where the attacker intentionally leaves infected USB drive or any optical disks at public places where anyone could pick it up due to curiosity and run the infected drive in their own devices and let the attacker access to the target information. Baiting only need a physical channel to get to the information which makes the human is the only operator for this technique (Weippl, et al., 2015). Baiting is also combination of social engineering and technical Subterfuge (Weippl, et al., 2013).

Vishing: The term "Vishing" is gotten from a blend of "voice" and "Phishing" and it is a sort of old-fashioned social engineering technique as the attacker use the phone to impersonate the interactive voice response of a company. In any case, with the ongoing progression in the IP communication system, it implies that there is a probability that a phone call could start as well as end at a PC anyplace on the planet. Also, the sum to be paid is insignificant, in this way making it bound to take part in Vishing tricks (Yeboah-Boateng & Amanor, 2014). Despite the fact that there are various vectors for the phisher to lead a vishing attack, it is vital to comprehend the sorts of information that are generally effectively picked up by the attacker utilizing IP communication administrations. Commonly, numeric data is all the more effectively presented by the victim when reacting to a vishing attack utilizing a versatile handset. The most significant data are Credit card details (including expiration data and card security codes), Account numbers and their corresponding personal identification numbers, birth date, Social Security numbers, and Passport numbers. However, the reason why it is important for the attacker to have this information is so they can control the victims' financial accounts, Purchase luxury goods and services, Identity theft, Make applications for loans and credit cards, Transfer funds, stocks and securities, Hide criminal activities such as money laundering, Obtain personal travel documents, and receive government benefits. The attacker can perform this type of attack via e-mail, mobile text messaging, voice mail, and live voice call (Ollmann, 2007).

Tailgating: Tailgating is another act of social engineering attack where the attacker basically follows an authorized employee to enter secure area for the authorized people only to steal private data (Ivaturi & Janczewski, 2011). In this scenario, the attacker will not only need to follow the employee to enter the secure area, but the attacker needs to do exactly what the employee does like wearing a uniform, communication, and then manipulate the human to enter the area by utilizing technical communication skills. Furthermore, the attacker must know the organization details and have the ability to communicate with the technician and have technical knowledge. That is the reason why it is also considered a partial technical attack (Maan & Sharma, 2012).

Pretexting: Pretexting is another type of social engineering of making and utilizing a well-prepared situation to induce the victims to deliberately uncover data or perform activities. In the business field, the attacker impersonates authorized organization and persuade small or new companies to unveil costumer information (Burd, et al., 2011). Pretexting is used in different aspect of life such as, sales, doctors, lawyers, and therapist or job that can create trusted scenario where the victims can reveal information. The attacker usually relies on targets personal or emotional attachment and that motivate the attacker for example, to create a website and pretext to fund cancer research center or fund natural disaster victims. The attacker must convince the target people to believe them as they use this tool to make the scenario more realistic such as, uniform, business card, and magnetic signs for vehicle (Hadnagy, 2010).

Quid quo pro: In this type of attacks, it requires a communication between the attacker and target to disclose information the attacker not supposed to have as the attacker attempt to make the conversation as friendly and comfortable for the target as much as possible so the attacker can ask about vulnerable data from the target and even when the attacker get the data, the conversation will continue to be friendly so the target do not subsect the attacker purpose (Mouton, Leenen & Venter, 2016). For example, the attacker can impersonate a technical support and pretend that the target is facing a problem and the attacker trying to solve the problem (Breda, Barbosa & Morais, 2017)

3. METHOD

This paper summarize different social engineering attacks mechanisms by reviewing different literature. Table 1 is summarizing the channel, operator, and type of each social engineering attack (Mas'ud, et al. 2011).

Table 1. Characteristics of Social Engineering attacks

		Phishing	Spear phishing	Baiting	Vishing	Tailgating	Pretexting	Quid pro quo
channel	**E-mail**	✓	✓		✓			✓
	Instant messenger	✓	✓					✓
	Telephone, voIP	✓	✓		✓			✓
	Social network	✓	✓					✓
	Cloud	✓	✓					
	Website	✓	✓					
	Physical	✓	✓	✓		✓	✓	✓
Operator	**Human**	✓	✓	✓	✓	✓	✓	✓
	Software	✓	✓		✓		✓	
Type	**Physical**			✓		✓	✓	✓
	Technical					✓		
	Social				✓		✓	
	Socio-technical	✓	✓	✓				✓

4. SOCIAL ENGINEERING AND NEW TRENDS

Field of computer is rapidly changing and new trends been discussed recently in conjunction with social engineering, such as: Big Data, Data Science, Cloud Computing, and Artificial Intelligence, in addition to the recent pandemic COVID-19

4.1 Big data and Social Engineering

With the emerge of big data, cybercriminals are focusing on collecting sensitive information of the users to have a business of these data such as selling in illegal markets (Salahdine, & Kaabouch, 2019).

The fast development of the Internet has carried with it an outstanding expansion in the sort and recurrence of cyberattacks. Some notable cybersecurity solutions are set up to defend against these attacks. In any case, the age of Big Data over computer networks is quickly rendering these traditional solutions obsolete (Mahmood, & Afzal, 2013)

Within the generation of big data, social engineering is highly expected to be more feasible Atwell, Blasi, & Hayajneh, 2016)

4.2 Cloud Computing and Social Engineering

Cloud computing, like other areas of information technology, has a number of security issues that must be addressed. These

risks include those associated with policy and organization, technical risks, as well as legal and other risks. Cloud computing is a collection of technologies, processes, people, and commercial structures (Jalamneh & Khder, 2021). As with any other technology, process, person, or commercial structure, the cloud is not without vulnerabilities. The following are some of the cloud's vulnerabilities, as well as some of the open issues and threats that require immediate attention: Vulnerabilities in Common Technology Data Breach, Internet Protocol, Denial of Service (DoS), Injection Vulnerabilities, Business Model Changes, Abusive Use, Malicious Insider, and Availability – When combined with social engineering or browser-based attacks, any vulnerability in a cloud provider's API or interface poses a significant risk Management. (Ramachandra, G. et al, 2017). In addition, social engineering can be a main threat to cloud computing by using account hijacking and Weak Authentication and Identity; while computers and electronics play a larger role in modern IT security, human error is still one of the weakest links. Human error is amplified in the cloud, as compromised credentials can cause havoc across applications and data. Hackers can steal credentials and thus hijack cloud accounts through phishing, fraud, and other forms of social engineering. Administrators should provide security education and certification to users, as well as develop and implement clear acceptable use policies and other security best practices. (Suryateja, 2018).

4.3 Data Science and Social Engineering

Data science is a combination of several disciplines that aims to get accurate insights from a bunch of data, develop the technology, and algorithm to solve the complicated problems analytically (Khder, et al, 2021). The vulnerability of social network members becomes a social networking issue as a result of their high and huge participation. Because a single vulnerable user can jeopardize the security of all friends, it is critical to understand how social network users' security can be improved. Data science different techniques easily cleaned, and analyzed the gathered short text messages from social networking site users. Additionally, phishing messages were created and sent to users via social engineering techniques. For user clustering based on their text messages, the K-means and Mini Batch K-means clustering algorithms can be used as an example. Data science can help in creating different specialized tool to automate the process of user clustering and phishing attacks. (Mažeika, D., & Mikejan, 2020). In addition, marketing social engineering can be another meaning of marketing intelligence which is refers to developing insights obtained from data for use in marketing decision-making, where data science play a big and vital role in that. (Chkoniya, 2020)

4.4 Artificial Intelligence and Social Engineering

Artificial intelligence is one of the Technology-based mitigation techniques that is used to enhance human-based mitigation techniques accuracy via inserting another security layer. Artificial intelligence systems can learn, adapt, and change parameters based on the circumstances (Salahdine, & Kaabouch, 2019). According to a study conducted by (Salahdine, & Kaabouch, 2019) artificial intelligence-based defense mechanisms are the most effective techniques to reduce the risk of social engineering attacks.

4.5 IoT and Social Engineering

The Internet of Things (IoT) is a rapidly developing technology. Home appliances, clothing, traffic lights, automobiles, cameras, and a variety of other items used by humans are likely to be connected to the Internet of Things. Every new technology comes with its own set of difficulties. One of the most difficult challenges of the Internet of Things is security. Security has always been a challenge on the Internet, but in the Internet of Things, security has become a much larger issue. For example, manipulating the traffic light system will have a negative impact on public safety and discipline. The Internet of Things is intertwined with the daily lives of human beings, which is carried out or controlled by users at all times and from any location. As a result, the Internet of Things will play an important role in human interactions. Individuals' social interactions and day-to-day activities can be influenced, resulting in the IoT being penetrated and security being compromised. Social engineering is not a new concept; SE is an old category that has been growing steadily for many years and has no end in sight. SE is effective because humans prefer to rely on their natural instincts to make decisions. Social engineers prey on human factors and take advantage of their trust in order to steal the desired information. Generally speaking, SE has an impact on social interaction (Ghasemi, et al. 2019). IoT that connects all these different kinds of everyday items and technologies will become a reality in the not-too-distant future. There have already been instances in which hackers have taken advantage of smart toys in order to steal personal information. As a result of hackers' quickness to exploit any weakness in cyber space, social engineering attacks on these devices, which have little or no security, are already a reality. (Gan & Heartfield,2016)

4.6 Social engineering related to Corona Virus Disease 2019 (COVID-19) pandemic

The pandemic has showed many vulnerabilities of humans in different aspect of life, including technological and end-user vulnerabilities that are wanted by the cybercriminals.

With COVID-19 outbreak, reported phishing attacks are up to 67% due to cybercriminals taking advantage of the pandemic to exploit the virtual environment of the organizations. As a result, unfortunately cybercrimes are rising dramatically as in April 2020 126 million malware and phishing emails related to COVID-18 were detected in one week only. Moreover, 240 spams are reported daily by Google's blog. In addition, phishing and hacking attacks have expanded 5 to 6 times during March (Naidoo, 2020)

5. PREVENTING SOCIAL ENGINEERING ATTACKS:

Data protection is very important and due to the advances of social engineering attacks, information security is essential. However, to prevent the attacks there must be a very well written security policy that technical and nontechnical can understand. Also, employees should be trained during the first months of their career and to aware and inform them about security. however, the organization must be secure by a whitelisting authorized website and user must maintain passwords that are changed every 60 days. Furthermore, not only the whitelisting authorized website is responsible to protect the organization but also the organization itself must check if their policy is being used the way it should by checking their network at least every month. In addition, the network must contain multiple layers of defense to protect the data like firewalls, Software like Intrusion Prevention Systems, Intrusion Detection Systems, web filters and Virtual Private Network, and Demilitarized Zones. Finally, it is critical for each organization to have security guide, secuiry cameras, and mantrap to protect the hardware from any physical attacks (Conteh & Schmick, 2016).

6. CONCLUSION

The security of data is critical in a recent society and despite the fact that the security around data is ceaselessly improving, the one powerless point is as yet the person who is cannot control procedures. This research explained the attack vector and characteristics of social engineering in general term.

7. FUTURE WORK

Extending this research to includes statics about the victims of each social engineering attack and evaluate the most target victim category in each of the attack vectors. Also, includes tactics that are used in social engineering attacks and more explanation of the social engineering taxonomy and prevention method for each of the attack vector

8. RECOMMENDATION

To help in spreading awareness towards social engineering attacks, the following recommendation are proposed for ministries of education: include social engineering topic in computer classes, conduct seminar for the student about the threat that could be carried through social network websites and e-mail or any channel for the social engineering attacks that are used daily by the teenagers. Moreover, for ministries of information affair: must make programs related to social engineering to increase society knowledge and aware the society from the danger that could follow the social engineering attacks.

REFERENCES

Atwell, C., Blasi, T., & Hayajneh, T. (2016, April). Reverse TCP and social engineering attacks in the era of big data. In 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS) (pp. 90-95). IEEE.

Breda, F., Barbosa, H., & Morais, T. (2017). Social engineering and cyber security. In em Conference: International Technology, Education and Development Conference.

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). On the anatomy of social engineering attacks—A literature-based dissection of successful attacks. Journal of investigative psychology and offender profiling, 15(1), 20-45.

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.

Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing attacks and defenses. International Journal of Security and Its Applications, 10(1), 247-256.

Chkoniya, V. (2020). Challenges in Decoding Consumer Behavior with Data Science. European Journal of Economics and Business Studies, 6(3), 77-87.

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.

Foozy, C. F. M., Ahmad, R., Abdollah, M. F., Yusof, R., & Mas'ud, M. Z. (2011). Generic taxonomy of social engineering attack and defence mechanism for handheld computer study. In Malaysian Technical Universities International Conference on Engineering & Technology, Batu Pahat, Johor.

Gan, D., & Heartfield, R. (2016). Social engineering in the internet of everything. Cutter IT Journal, 29(7), 20-29.

Ghasemi, M., Saadaat, M., & Ghollasi, O. (2019). Threats of social engineering attacks against security of Internet of Things (IoT). In Fundamental Research in Electrical Engineering (pp. 957-968). Springer, Singapore.

Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. Telecommunication Systems, 67(2), 247-267.

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

Ivaturi, K., & Janczewski, L. (2011, June). A taxonomy for social engineering attacks. In International Conference on Information Resources Management (pp. 1-12). Centre for Information Technology, Organizations, and People.

J. Hong, "The state of phishing attacks. Commun", ACM. vol. 55, no. 74, (2012).

Jagatic, T., Johnson, N., Jakobssen, M., and Menczer, F. 2007. "Social Phishing," Communications of the ACM (50:10), pp 94-100.

Jakobsson, M., & Myers, S. (Eds.). (2006). Phishing and countermeasures: understanding the increasing problem of electronic identity theft. John Wiley & Sons.

Jalamneh, A.A, & Khder, M.A. (2021). Challenges of Implementing Cloud Computing in the Arab Libraries Environment. Information Sciences Letters, 10(1), 10.

Khder,M.A,Fujo,S.W and Sayfe,M.A. (in press). A Roadmap to Data Science: Background, Future, and Trends.Int. J. of Intelligent Information and Database Systems.

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). ACM.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, 113-122.

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.

Maan, P. S., & Sharma, M. (2012). Social engineering: A partial technical attack. International Journal of Computer Science Issues, 9(2), 557-559.

Mahmood, T., & Afzal, U. (2013, December). Security analytics: Big data analytics for cybersecurity: A review of trends, techniques and tools. In 2013 2nd national conference on Information assurance (ncia) (pp. 129-134). IEEE.

Mažeika, D., & Mikejan, J. (2020). Investigation of User Vulnerability in Social Networking Site. In Data Science: New Issues, Challenges and Applications (pp. 219-234). Springer, Cham.

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

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. European Journal of Information Systems, 1-16.

Ollmann, G. (2007). The vishing guide. h ttp://www. infosecwriters. com/text resources/pdf/IBM ISS vishing guide GOllmann. pdf, IBM, Tech. Rep.

Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A comprehensive survey on security in cloud computing. Procedia Computer Science, 110, 465-472.

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

Suryateja, P. S. (2018). Threats and vulnerabilities of cloud computing: a review. International Journal of Computer Sciences and Engineering, 6(3), 297-302.

Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., ... & Margolis, D. (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). ACM.

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.