Journal of Computing, Science &Technology
https://focjournal.unidel.edu.ng/
editorjcst@unidel.edu.ng

ISSN: 3043-6818 Print

https://focjournal.unidel.edu.ng

Social Engineering and Personal Data Security: Attacker Perception, Security: Attacker Perception, Motivation and Mechanism

Richard Omoefe Oveh[1]
[1]Department of Information and Communication Technology, University of Delta Agbor, Delta State, Nigeria
richard.oveh@unidel.edu.ng[1]

Corresponding Author's Email: richard.oveh@unidel.edu.ng

ABSTRACT

Article Info
Date Received: 14-01-2024
Date Accepted: 12-04-2024

Keywords:
Social Engineering, Social Engineering attack, Technological defense, Security

Social Engineering is a psychological means of manipulating human weakness to steal sensitive data / information for the purpose of harm or theft. Criminals are now resorting to more fashionable social engineering attacks that take advantage of the weakest link in the chain which is humans as a result of increased technological defense. Despite the negative effects, it has been claimed that the attacks' alleged influence on people has gone unnoticed. In order to examine both the attacker's and the victims' perspectives, this paper aimed to ascertain the attacker's viewpoint, motivation, and mechanism. Mixed methodology was used for this research using qualitative and quantitative methods. Questionnaire was used for the quantitative method, while interview was also conducted to obtain further information. Fourteen (14) persons were randomly selected and used as our case study for this research. The result suggests a gender bias in the attacker and the victim, with the males being the predominant attacker with the females being the victim. The result also showed that despite the attackers knowing the consequences of their actions continue in their trade. It was further observed that despite the attacker's being significantly educated, it was not sufficient to dissuade them from committing crime motivated for illegal gains with security and other consequences. A framework was then proposed to mitigate the actions of social engineering using a social engineering machine learning evaluator mode.

1.0 INTRODUCTION

The word "social engineering" has no formal definition [1]. Social engineering involves manipulating human errors or weakness to collect private data/ information in other to gain to valuables. It is carried out in an unsuspecting manner and it is built on people's perception and actions. Increase in technology defense has pushed cyber criminals to adopt social engineering technique due to humans being labelled the weakest link [6]. [5] Defines it as the induction of victims to expose confidential and classified data exploiting innocent instinct. [4] argued that social engineering is the simplest method to gather data by exploiting human weakness. [7] defines it as a variant of cyber-attack where sensitive information is obtained by manipulating people. They opined that it's extremely effective because of it's persuasive and deceptive nature. The major goal of social engineering is for sabotage to cause harm or theft. [2] argued that attacks via social engineering that were targeted at a particular person or group of people have received comparatively little study. The impact of such attacks on people has gone unrecognized despite the detrimental implications on the victim's financial and emotional wellbeing [2]. Social engineering has become a source of concern as there is a present rapid increase in its attacks against networks, which has a resulting weakening effect in the cybersecurity chain [9]. The technique for social engineering is shown in Figure 1.

The methods of social engineering attack include phishing, baiting, spoofing, scareware, watering hole, cache poisoning, tab nabbing, tail gating, etc. The weakest link that can be manipulated to manipulate int o disclosing sensitive information has been found to be hu mans. Due to the inability of technology to completely avo id psychological manipulation, anyone can become a victi m of social engineering attacks [3][2]. Personal data security is the habit of protecting personal and sensitive information from an unauthorized access or theft [8]. The strategies for personal data security include: Using reliable software, updating your software, researching the origin of emails, setting your spam email settings to high, having a personal policy against social engineering attacks, using two-factor or multiple factor authentication, avoiding using

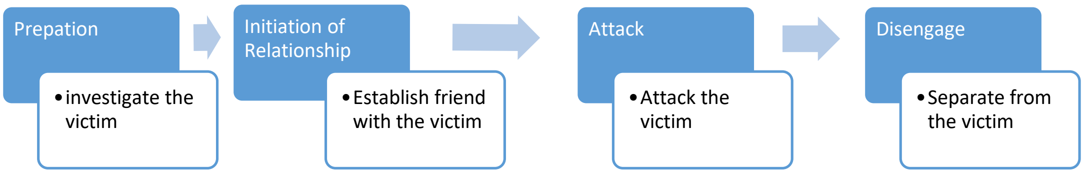
Prepation
• investigate the victim
Initiation of Relationship
• Establish friend with the victim
Attack
• Attack the victim
Disengage
• Separate from the victim

Figure 1: Social Engineering Technique

the same password repeatedly, minimizing your digital footprint on social media, and avoiding using untrusted websites are all examples of common security practices against social engineering attacks. This paper seeks to determine the attackers' perception, motivation and mechanism, with a view to exploring the perspective from the attacker and victim.

1.2 Materials and Methods

Mixed methodology was used for this research using qualitative and quantitative tools. Questionnaire was used for the quantitative method, while interview was also conducted to obtain further information. An open ended questionnaire was used for data gathering. The open ended questionnaire gave room for the respondents to add other relevant information. The questionnaire was divided into two (2) sections the first part was on the bio data of the respondents, while the second part contained the social engineering act. Fourteen (14) persons were randomly selected and used as our case study for this research.

2.0 Results

The questionnaire bio data is shown in Table 1. The responses show that the attackers are predominantly males with 100% response. It also showed that the social engineering attackers were well aware of their act and the consequences of their actions if caught. It was also observed that majority of the respondents were educated (BSc, HND, OND, SSCE), which suggests that education was not sufficient to dissuade people from committing crime motivated for illegal gains. .

Table 1: Respondents Bio data

s/n	Question	Response	Frequency (%)
1	Sex	Male	100
		Female	0
2	Crime Awareness	Yes	100
		No	0
3	Literacy Level	Graduate (BSc/HND)	57.1
		OND	21.4
		SSCE	21.4

It was observed from Table 2 that the medium of attack was principally through social media sites and business related transactions, using techniques enveloped in deceit. Interestingly it was observed that there is an informal but effective means of learning the implicit act of social engineering through a school or a friend. The major motivation was the need for money and peer pressure. They attributed success to be the presence of money. This orientation is a major concern that calls for proper attention and correction. Their targets was seen to be humans with a major focus on the female folks and the category that tends to be most vulnerable. Another orientation that calls for attention as shown in Table 2 is the perception that the ill-gotten resource is a blessing instead of the bane to the society that it brings. The respondents erroneously see their crime as the solution to gang related deaths and unemployment. Their continuous presence and successes of their acts is the mastery of the act deceit towards their victims, security agents and their false identity. Figure 2 shows the resulting hierarchical representation obtained from Table 2.

Table 2: Questionnaire Responses

s/n	Questions	Interview Extract	Code
1	How do you source for your clients?	• Dating sites • Social media (Facebook, YouTube, Instagram} • Adverts on social media • Crypto-investment website • Randomly • Binary investment • Phone, calls and sms	Attack Medium
2	What technique(s) do you use?	• Baiting • Dating • Crypto investment • Ads on social media • Relationship • Deceit • Social media account hacking	Attack Techniques
3	How did you learn the act (Social Engineering)?	• On the street / friends • Fraud school	Training Source
4	What influenced you into the act (Social Engineering)?	• My friends had cash so I had to join • Lack of job • Pressure from friends • All my friends are into it • Lack of money	Social Influence
5	What is your motivation for the social engineering?	• Money • Poverty • Friends success • Fear of being broke	Attack Motivation
6	Who are your targets and why?	• Single foreign western women that are lonely • Anyone • Women in their 40's and 50's	Target
7	What impact has social engineering had on the economy?	• Fraud is on the rise it has reduced gang related deaths	Attack Impact

		• Don't know • We don't need jobs • Self employment • It has gotten many off the street	
8	How do you manage to avoid security agencies?	• I use two device as I leave my work tools at home • Having a false business setup to pass as my source of income • I have employer identity card • I keep low profile • I pay security officers	Attacker Secret

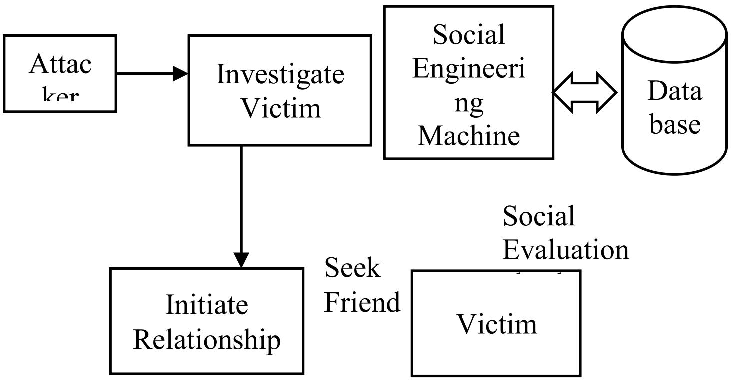

Figure 3: Social Engineering Framework

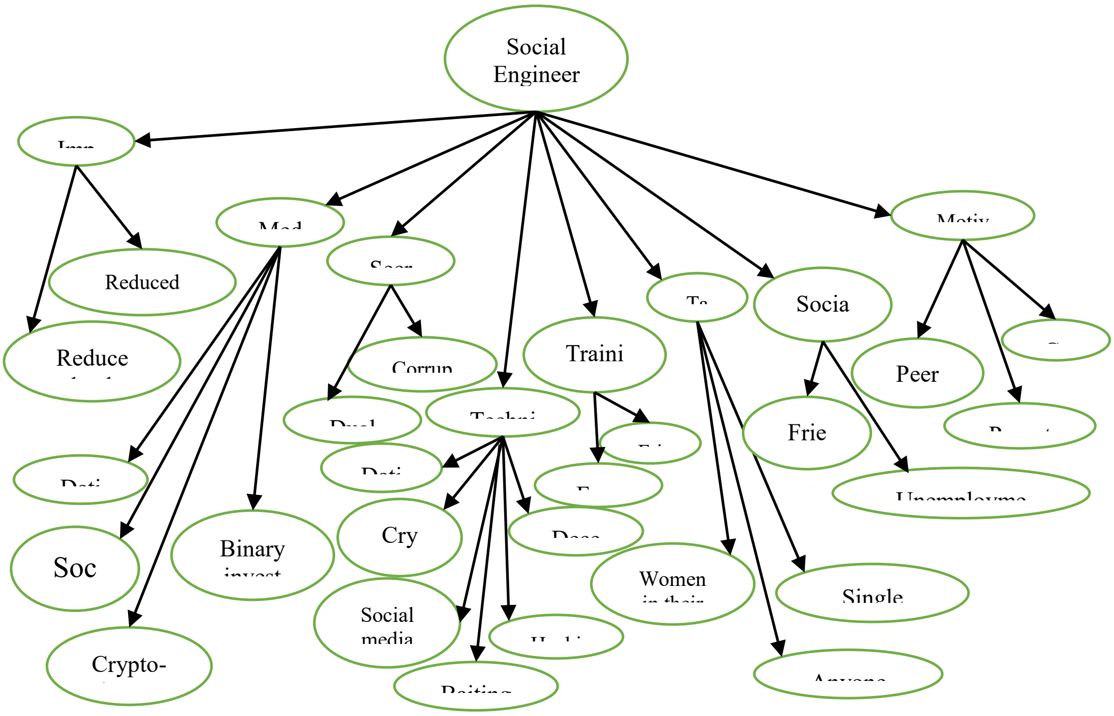

Figure 2: Hierarchical Diagram of Social Engineering Attack

3.0 DISCUSSION

The responses from the respondents which can be seen in their Social engineering attack successes suggests that the focus of their attack is on humans which has been identified to be the weakest link in the security chain as identified by [2][3]. This necessitates the need for the proposed social engineering framework in Figure 3. From the proposed framework in Figure 3, the attacker initiates the process of social engineering from investigating the victim to initiating relationship with the victim. The victim then initiates a social evaluation check from a social engineering machine learning model which feeds itself from a database containing repository of attacks. The proposed framework's machine learning model is trained from features of previous attacks and it is able to predict subsequent attacks hence the need for a check by the victim. The response from the machine learning model determines the next line of action of the victim whether to disconnect or create a relationship.

4.0 CONCLUSION

Increase in defense technology has pushed criminals to a more trendy attack of social engineering which manipulates the weakest link in chain which is humans. The purported impact of this attacks on people has been said to be unrecognised despite the detrimental implications. This paper sought to determine the attacker's perception, motivation and mechanism, with a view to exploring the perspective from the attacker and victims. Mix methodology of questionnaire and interview was adopted for data gathering. The result showed a gender bias in the attacker and the victim, with the males being the predominant attacker with the females being the victim. The result also showed that despite the attackers knowing the consequences of their actions continue in their trade. It was further observed that the victims being significantly educated was not sufficient to dissuade them from committing crime motivated for illegal gains. A framework was then proposed to mitigate the actions of social engineering using a social engineering machine learning evaluator mode.

REFERENCES

[1.] Wang, Z., Sun, L., & Zhu, H. (2020). Defining Social Engineering in Cybersecurity. IEEE Access, 8, 85094–85115. https://doi.org/10.1109/ACCESS. 2020.2992807

[2.] Bhusal, C. S. (2021) Systematic Review on Social Engineering: Hacking by Manipulating Humans. *Journal of Information Security*, 2021, 12, 104-114, Available at SSRN: https://ssrn.com/abstract=3821594

[3.] Bodnar, D. (2022) Social Engineering and How to Prevent It. Retrieved July 6, 2022, from https://www.avast.com/c-social-engineering

[4.] Conteh Y.N. and Schmick P.J. (2016) Cybersecurity: risks, vulnerabilities and countermeasures toprevent social engineering attacks, International Journal of Advanced Computer Research, 6, 23-31

[5.] Dey, P. K. (2016) Prashant's algorithm for password management system, International Journal of Engineering Science. 2424

[6.] Breda, Barbosa and Morais (2017) SOCIAL ENGINEERING AND CYBER SECURITY. Available at: https://www.researchgate.net/publication/315351300_ SOCIAL_ENGINEERING_AND_CYBER_SECURIT Y . Accessed: 5 October 2022

[7.] Allen, J. and Firch, J. (2022) Social Engineering: What Is It And Why Is It Effective? Available at: https://purplesec.us/learn/why-social-engineering-works/ Accessed: 5 October 2022

[8.] Poza, D. (2021) *what is Data Security? Learn Data Security Best Practices*. Retrieved October 10, 2022, from https://auth0.com/blog/what-is-data-security/

[9.] Salahdine, F. and Kaabouch, N. (2019) future internet Social Engineering Attacks: A Survey. Journal of Future Internet. Available at: https://doi.org/10.3390/fi11040089</div>