SOCIAL ENGINEERING PRESSURES IN NIGERIA INSTITUTIONS: WHY STUDENTS ARE THE MAIN TARGETS?

BY

Ismail Olaniyi Muraina:
Computer Science Department, College of Information and Education Technology, Lagos State University of Education, Lagos; E-mail:niyi2all@yahoo.com

Moses Adeolu Agoi:
Computer Science Department, College of Information and Education Technology, Lagos State University of Education, Lagos

Akeem Ademola Adedokun:
Computer Science Department, College of Information and Education Technology, Lagos State University of Education, Lagos

&

Bashir Ayinde Oyeniran:
Computer Science Department, College of Information and Education Technology, Lagos State University of Education, Lagos

Abstract

The great advancement of digital processing and communications has made connectivity and communication between and among humans more accessible, current, and timely. However, social engineering threats and challenges have emerged as one of the most sensitive and critical issues confronting not only the business counterparts but also targeting students of higher learning through which their parents and relatives are falling victims. As revealed from previous studies, threat actors are currently increasing using social engineering stratagems or tactics in the school environment to track down their relatives by luring those involved outrageously utilizing psychological manipulation techniques to circumvent technical security systems. Despite the usefulness of technologies everywhere and every day, there are some disadvantages attached to them and chief among these disadvantages is social engineering threats. This study addresses the major challenges social engineering threat can pose to students, parents, teachers, and school managers which could lead to losing valuable personal or private information, finances or even lives as a result of the physiological and psychological consequences of social engineering attacks. The study as well looks at how the issue of social engineering threats could be ameliorated if not abolished in Nigerian institutions. Higher institution students formed the target population of the study where 200 students already in higher institutions were asked via Google form to solicit their experience or witness or opinion towards the effect of social engineering threat on their families and relatives coupled with the interview conducted to find out students' awareness and possible ways to avert the situation in future- the interview involved 20 students on phone contacts. Both face and content validities were applied before the final draft of the items were uploaded into Google form for administration. The instrument was considered reliable after collating two separate copies of the results to Chronbach's Alpha statistical approach with a 0.77 reliability index. The major findings of the study have a connection with the age, exposure, and ignorance of most of the students when getting into higher institutions; in the same vein, most students do look at various opportunities inherent in the use of technologies and neglecting the side effect of any new technologies introduced. Conclusions: a series of orientation programmes should be organized at departmental, college/faculty, and institutional levels to sensitize them on care attached to technology use and keeping personal or private information safe from whomever they don't trust to avoid breaching their family security and privacy.

Keywords: Social Engineering Threat, School Environment, Technology Use, Attacks

Introduction

The social engineering threat attacks are becoming too rampant in the educational field every day. There is an incoming threat in the educational field that if not looked into can result in a dangerous attack that can victimize students and educational institutions, especially those who are from third world countries. Social engineering is a term that encompasses a broad spectrum of malicious activity (Blancaflor & Banzon, 2021). It involves preying off human psychology and curiosity to compromise victims' information. With this human-centric focus in mind, organizations must help their employees counter these types of attacks. Ghafir; Saleem; Hammoudeh; Faour; Prenosil; Jaf; Jabbar & Baker, (2018) define social engineering as the art of exploiting the naïve or inexperienced youths of unsuspecting individuals and taking advantage of their novelty to the security alertness or their weaknesses to convince them to comply with one's desire. Therefore, Ghafir et al., (2018) suggested not to rely on an organization's technical security shortcomings to break into its networks because social engineers use employees (Teachers in the school) and customers (students) to mislead them into compromising the system or turning over sensitive and vital information. Ajaegbu; Adesegun; Adekunle & Awodele (2013) observed that social engineering attack leverages on human mind or emotional desires rather than technological-based attacks. In their study, they observed the level of students' awareness of social engineering threats in Ogun State Nigeria. The results obtained showed that the level of awareness of social engineering threats was so poor. So, they advised more campaigns to gain the attention of people towards the danger posed b the malicious acts. Different authors with different views of the definition of social engineering; Kalnin; Purin, & Alksnis, (2017) see social engineering as a way to manipulate individuals and organizations to divulge valuable and sensitive information in the interest of attackers. Pokrovskaia, (2017) said that they get people trapped in malicious activities by using human interactions to influence a member or person psychologically to divulge confidential information or to break the security procedures to get what they want. To Aroyo; Rea; Sandini & Sciutti, (2018) cyber criminals such as social engineers choose these attack systems when they observe that there is no way to hack a system with no technical vulnerabilities. According to Pilette, (2021) social engineering can be said to be the art of manipulating someone to divulge sensitive or confidential data or information, which could be used in fraudulent acts. The social engineering style of operating is a bit different from its counterparts like cybercrime or cyber-attacks. Social engineering does not need or rely on security vulnerabilities to have access to any information or unauthorized devices or networks but targets human beings' vulnerabilities to operate. As a result of this, it is also called human hacking. Pilette, (2021) observed two major goals of any social engineer or social engineering attackers: 1. To obtain valuable information, 2. To obtain money.

The below research questions guide the study:
Is there any significant connection that students' age, exposure, and ignorance have concerning social engineering attacks?
Is there any significant importance in sensitizing families, friends and schoolmates of the dangers posed by social engineering attacks?
Are there any significant tricks that must be learnt to avoid being attacked by social engineers?
Who is in the best stance to stop the social engineering threats in the school environment?

Concept of Social Engineering

According to Maan & Sharma, (2012) social engineering could be seen as an attack on human psychology by using some technical skills or technology to succeed in their tricks. Social engineering is defined by Hasan, Prajapati & Vohara, (2010) as a process of deceiving people into giving away access or confidential information with the use of persuasion. The authors considered social engineering as the most powerful attack because no hardware or software could be used to prevent it. McDowell, (2007) defined social engineering with relevant examples, when he defined it as a euphemism for non-technical or low-technology means used to attack information systems such as the use of impersonation, tricks, lies, bribes, blackmails and threats. White (2015) observed that the social engineering act does not require sound technical knowledge to be successfully carried out its attacks. Instead of this, social engineering

preys on common aspects of human psychology like shyness, curiosity, courtesy, greed, apathy and other ones. Social engineering is the art of getting victims to compromise information. It targets humans with access to information then manipulates the information and divulges confidential information or carries out malicious attacks via influence and persuasions (Krombholz et al., 2014). Therefore, social engineering is referred to as the manipulation of individuals to induce them to carry out unlawful acts or divulge information that can be of use to an attacker. It must be noted that social engineers are very creative and highly metamorphosed their actions or tactics to take advantage of new situations or technologies.

Syed (2020) pointed out that young children below 20 years of age were a common target for the attackers because most of them lack knowledge regarding threats on the use of sophisticated devices. Most of these students often create free accounts on the internet without any permission from their parents or guidance. The use of weak passwords attracts the attackers' attention and can break into the account easily and gain access to their parents' personal information cheaply. Sadiku, (2016) defined social engineering as an umbrella term used for computer exploitations that make use of a series of strategies to manipulate a user or victim.

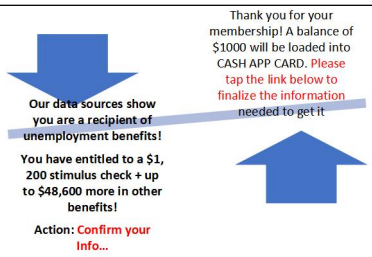
Conclusively, social engineering is manipulating a person into knowingly or unknowingly giving up information; essentially 'hacking' into a person to steal valuable information. It is a way for criminals to gain access to information systems. The major purpose of social engineering is usually to secretly install spyware, and other malicious software or to trick persons into handing over passwords and/or other sensitive financial or personal information. Social engineering is one of the most effective routes to stealing confidential data from individuals and organizations.

Social Engineering Types

Social engineers are those who leverage their skills in computing to infiltrate guarded devices (phone calls and other media) and compromise sensitive data. They go a long way to exploit human psychology and eventually trick them into handing over access to the family's or organization's sensitive information. The common types are discussed in table 1.

ISSN 2384-7662
E-ISSN 2705-2508

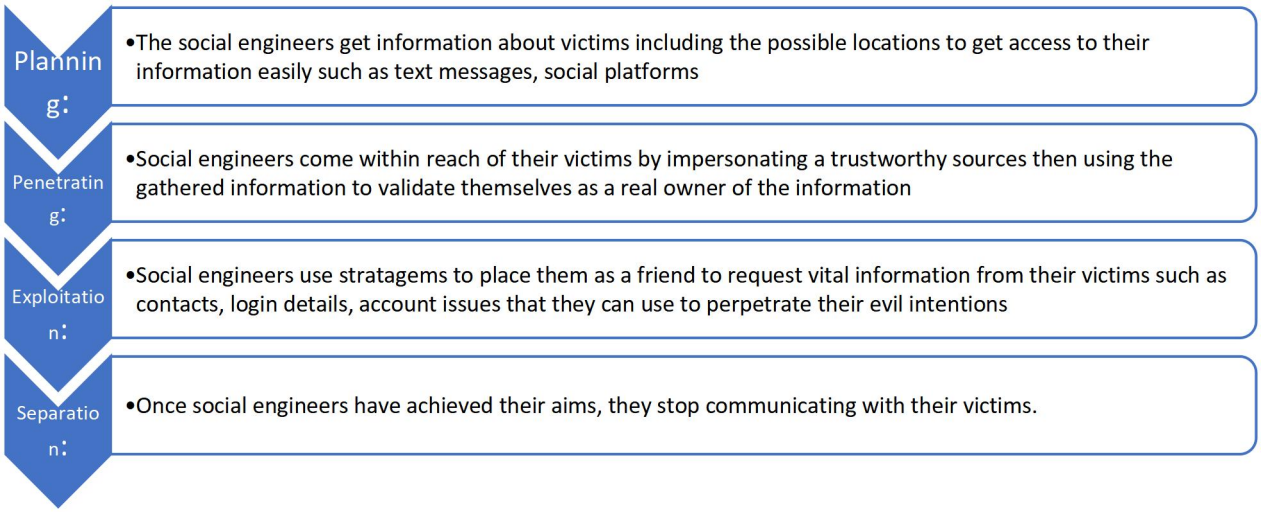
Table 1: Different Types of Social Engineering

Phishing	Social engineers use phishing to obtain personal information such as names, addresses, account numbers, and security numbers. Also, use shortening or misleading links to redirect users or victims to suspicious sites that leverage fears or a sense of urgency to get the victim into responding quickly to their traps		SOCIAL ENGINEERING
Pretexting	In this type, social engineers focus on creating a pretext or a fabricated situation to steal the victim's personal information. The major method in this type is the use of impersonation.		
Baiting	This type uses a target or promise of valuable items to entice victims such as a free offering of music, cards, and movie to get the victim's login credentials.		
Quid Pro Quo	This type is similar to baiting because attackers promise items in exchange for any information shared or provided for use.		
Tailgating	This type uses impersonation to pretend as an authorized one to gain access to the organization or school's information		

Most common ways social engineers manipulate to attack students, teachers, and other school managers

ISSN 2384-7662
E-ISSN 2705-2508

Table 2: Social engineering manipulative ways



Secrete Languages Social Engineers use to attack

Social engineers are so bold to the extent that they communicate with victims in plain sight. Some of the following tactics give clues to their actions:
i. One needs to be very careful when friends, co-workers, relatives, boss, and coursemates (somebody you trust) send them very conspicuous messages with malicious links or downloads. Try to verify from the friends before moving further
ii. One should try to control his/her emotions because social engineers are very good at stirring up our emotions such as curiosity, happiness, excitement, and anger. If care is not taken seriously one may fall into the net through emotional trigger actions.
iii. In most cases, social engineers do request information from their victims urgently, so one should think twice before reacting to such requests.
iv. One should be sensitive to some messages that look like chances to win or qualify for a promo. Not all that glitters is gold. So, don't try to ripe from where you did not saw.
v. At times, social engineers might reach out to you pretending to be messaging or calling you from a company or an organization to render to you any assistance regarding the problem you are facing right away (Similar to a tech support scam). Try to desist from supplying them with vital information that could lead to the destruction of your accounts and life
vi. Once you suspect that the person is a social engineer, try to request their identity through video calls so that you will see the person.

How to avoid being attacked by a Social Engineer
As students, teachers and other school managers, the best way to avoid being attacked by the so-called social engineers is to educate all the people concerned about the risks, the alarming, and remedies.
Below are some of the tips:

ISSN 2384-7662
E-ISSN 2705-2508

Table 3: Students' precautions to prevent social engineers' tricks

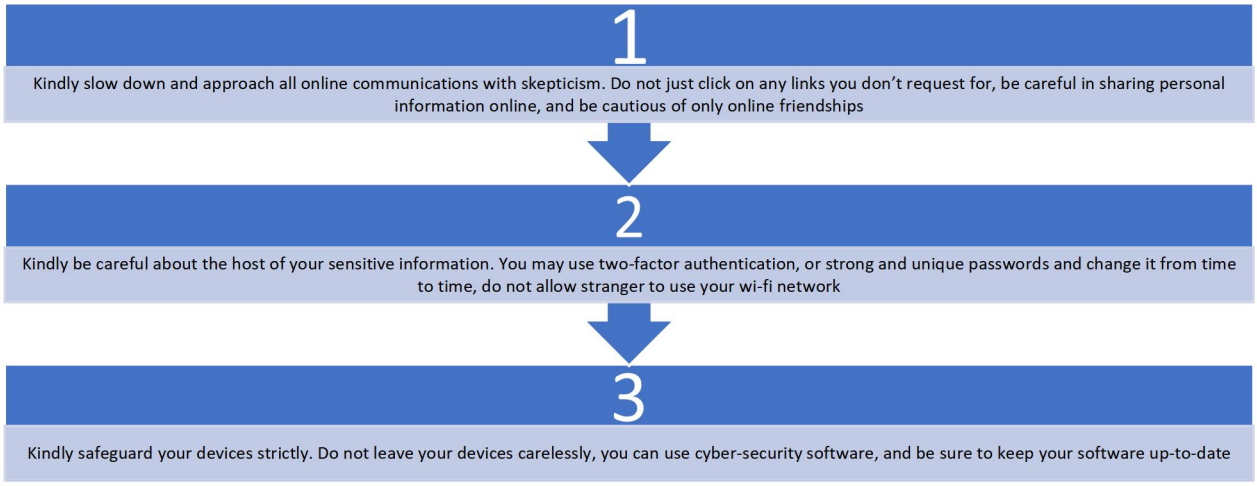


Table 4: Three important qualities to be learnt by students from falling into the social engineering trap

	Beware Everyone needs to beware of phishermen, vishers and other scammers. They are everywhere. So, keep personal information private
	Be Aware Study the tricks of social engineers like asking for urgent information, wire transferring or clicking on links
	Share Be the one to share information regarding social engineering threats to your friends, families, and well-wishers

As shown in table-4, every individual needs to beware of different types of scammers or social engineers and their dubious acts to keep all personal information private and safe; at the same time, individuals should be aware not just clinking any links or request from whoever they don't trust or at times asking them any information urgently or in haste. Finally, since social engineers are on every corner, it is more advisable to inform all our children, relatives and family members about the social engineering attacks and tricks by also educating and unveiling all their secretes

ISSN 2384-7662
E-ISSN 2705-2508

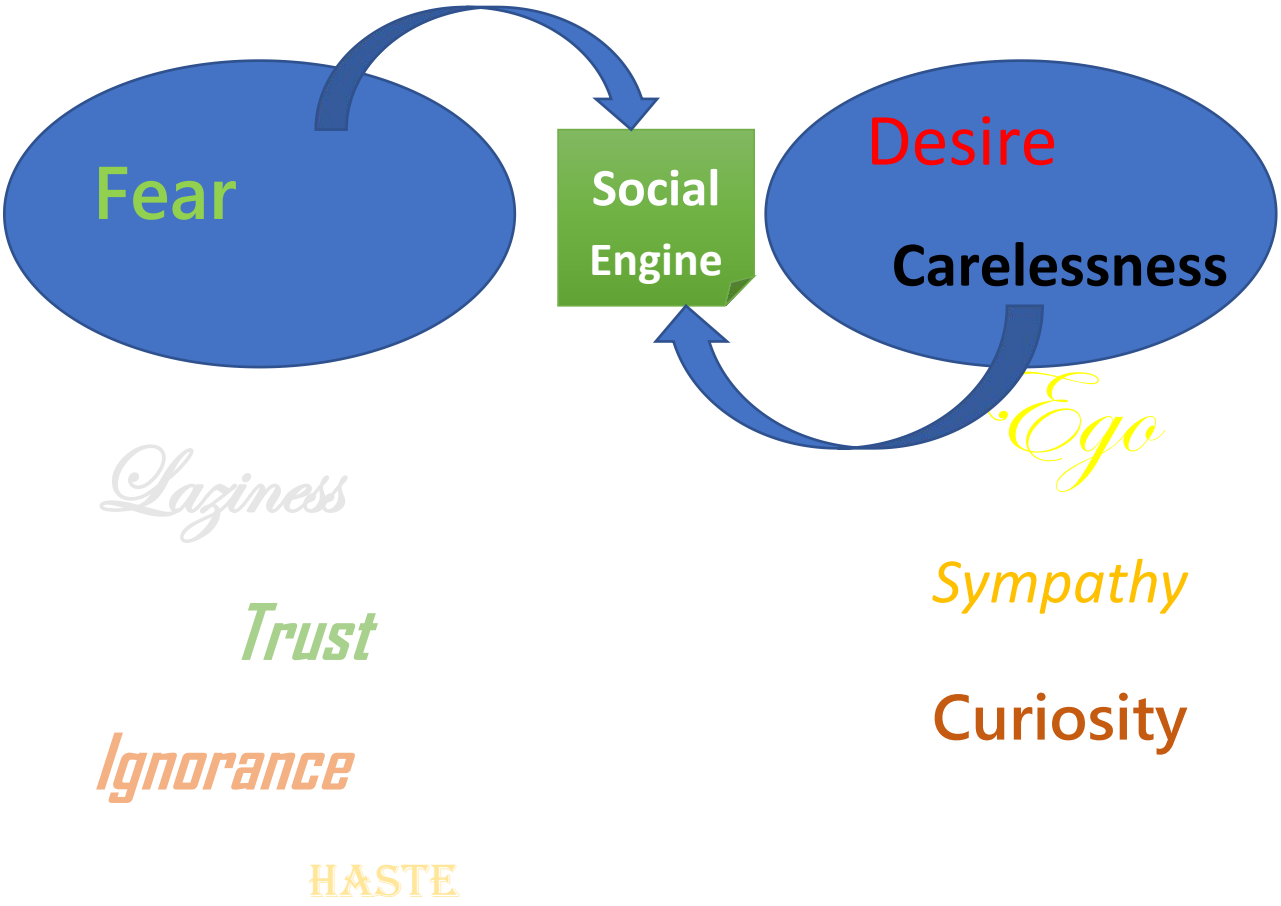


Figure 1: Social engineering tools to trick victims

There are so many tricks social engineers use to prey on victims; these include Laziness, trust, ignorance, haste, fear, carelessness, ego, desire, sympathy, and curiosity as it is shown in figure-1. Social engineers can use any of the aforementioned tricks especially when their target is young children; they know that students who are for the first time being exposed to a higher institution environment are ignorance of so many things, so they easily trust whoever comes their way in seeking knowledge, from there they will instil fear in them and get them attacked seriously.

Related Literature

Blancaflor & Banzon, (2021) conducted a study to carry everyone along about the vulnerability in gathering data from educational institutions. The survey method was used to experiment by pretending that the information given to them was for academic purposes whereas to get their data for other purposes. Most of the students answered the survey. Through this approach, they were able to collect their information regarding email addresses, names, social media accounts and more. In the end, the study showed how vulnerable the educational field is to basic cyber-attacks and gave some informative recommendations on what to do. Social engineering has recently emerged as the most hideous issue facing the educational domain in the 21st century. Observations have shown that social engineers find attacking students especially easy after efforts were invested to penetrate their parents and other relatives proved abortive. Factors like the age of the students, their exposure, and their ignorance of information

sharing ethics are the underlying reasons why attacks are so common in school environments. As put by Arlitsch & Edelman, (2014) more attentions are focused on security and that is why cyber-security or social engineering threats have become a massive discourse in schools. The issue of social engineering threats and other related challenges has brought about so much research in recent times.

Gioe, Goodman & Wanless, (2019) also observed that security threats have emerged as a critical and attention-focused issue confronting many institutions in the 21st century. Alongside is the view of Shen, Chen & Su, (2017) who made it crystal clear that school have exposed their data and information to a range of nefarious cyber activities due to the sudden transformation of moving all the information to the internet services to ease student information management. According to Salahdine & Kaabouch, (2019), the glory brought by the advancements in digital communication technology has given room to the availability of personal and sensitive information online via social media networks and other online services which has made communication systems vulnerable and can easily be penetrated by malicious users through social engineering attacks. These attacks are aimed to trick family members, students, school teachers or managers into accomplishing actions that will attackers or at the time provide them with sensitive data that could eventually put the whole family or organization into serious problems.

Most previous studies are aware and observed the tricks usually employed by social engineering attackers, for instance, Nguyen & Bhatia, (2020) made it known that social engineering tactics include the use of psychological manipulation strategies to circumvent technical security systems. He suggested using a new approach to mitigating and stopping social engineering but the new approach was not mentioned in the end. Alsulami; Alharbi; Almutairi; Almutairi; Alotaibi; Alanis; Alotaibi & Alharthi, (2021) emphasized the social engineers' techniques used to manipulate users into either granting them access to various systems or disclosing their private and confidential data and information and the financial implication of social engineers attacks on organizations and how it is necessary for every organization to increase their awareness campaigns of the present of social engineering threats and a way to prevent it, especially in our schools. The study conducted by Alharbi et al., (2021) that aimed to provide a measurement of social engineering awareness in the Saudi educational sector, showed that only 34% of participants (158 out of 465 participants) had previous knowledge of social engineering approaches in the school system. It was suggested that training of staff and students could only be helpful to increase the awareness of social engineering attacks in schools

Materials and methodologies

A descriptive survey design was used. According to Voxco, (2022) the descriptive research design assists researchers to gain a deeper knowledge of the problem at hand. So, the use of the descriptive survey research approach accommodates both quantitative and qualitative data to give out relevant and accurate information. Young students in higher institutions formed the population of this study where 200 students were sampled: The whole 200 students were used for quantitative data while 20 students were used for the qualitative data. A questionnaire and structured interview instruments were employed to collect data from the participants. The interview lasted for about 15 minutes. In the interview process, a semi-structured, open-ended interview was developed from the literature, and eventually finalized. The instruments were subjected to content and face validities through colleagues and other experts in the field of computing and education. The instruments were confirmed reliable via Chronbach's Alpha as well as the use of copies of the interview instrument to describe a situation, to find out how it was performed and later got a good result of its description. Analysis was done using simple percentages and charts.

Results

4.1 Questionnaire Analysis

ISSN 2384-7662
E-ISSN 2705-2508

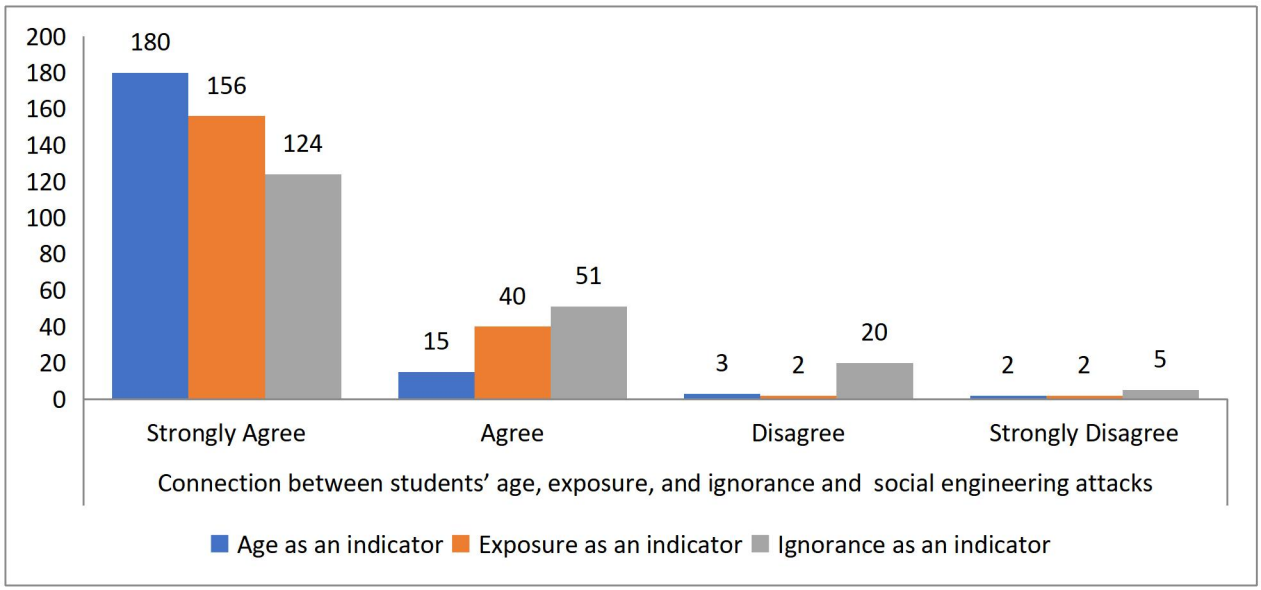


Figure 2: Connection between students' age, exposure, and ignorance and social engineering attacks

The study sets out to find the variable among age, exposure and ignorance that social engineers do use to attack students most. From figure-2, it was observed that 180, 56, and 24 respondents strongly agreed that social engineers use age, exposure of the students, and finally their level of ignorance to attack students. Meanwhile, the ages of the students were considered most often used to attack them because most of them could not decide independently.

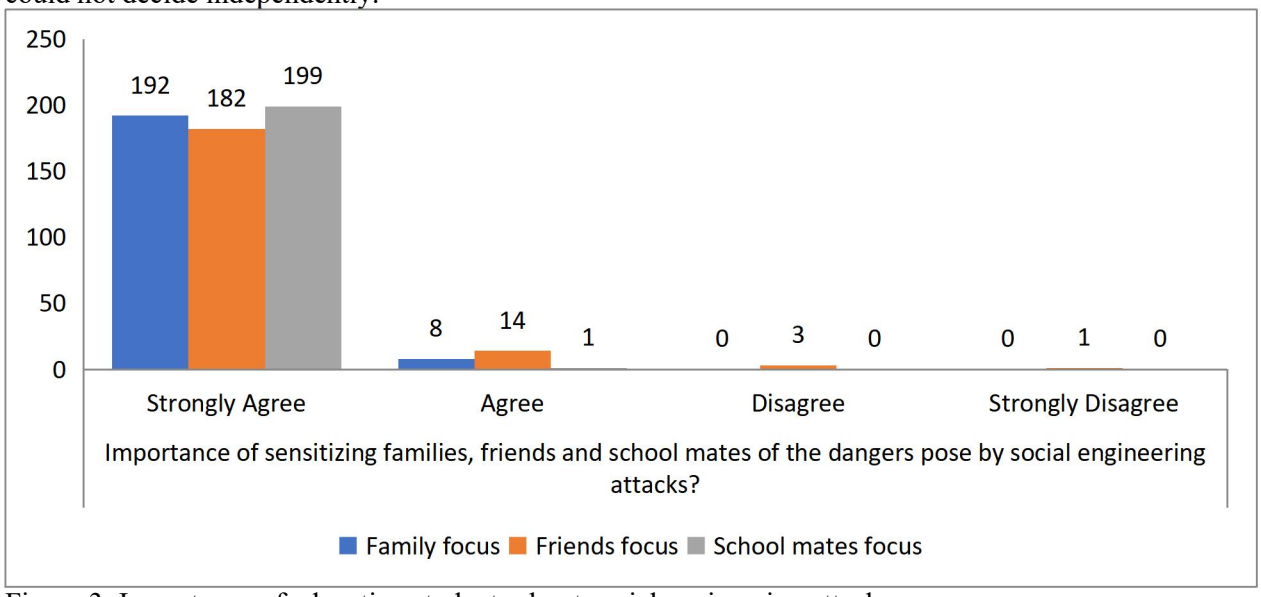


Figure 3: Importance of educating students about social engineering attacks

The study also sought the opinions of students regarding educating them on the dangers of social engineers in the school environments. Figure-3 showed that education should focus on schoolmates, then family members and friends with 199,192 and 182 respectively strongly agreed that educating students' mates, families, and friends are very essential in preventing social engineering attacks.

ISSN 2384-7662
E-ISSN 2705-2508

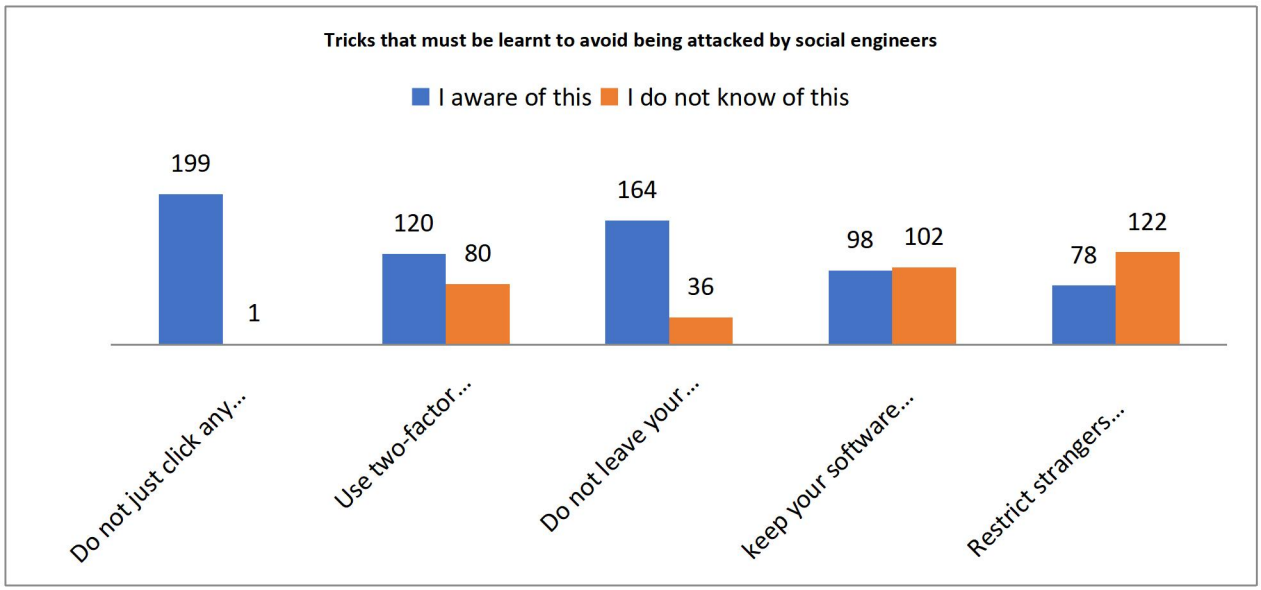


Figure 4: Social engineers' Tricks and way out

In checking the tricks used by social engineers, 199 respondents agreed and were aware to not just click on any link they don't trust, 164 respondents agreed and aware not to leave their devices carelessly, 120 participants agreed and aware to use two-factor authentication passwords to protect their systems; while 102 respondents did not aware that it is necessary to keep the software of their devices up-to-date for security purposes; also, 122 participants did not aware that it is good to restrict strangers from gaining access to wi-fi networks just anyhow.

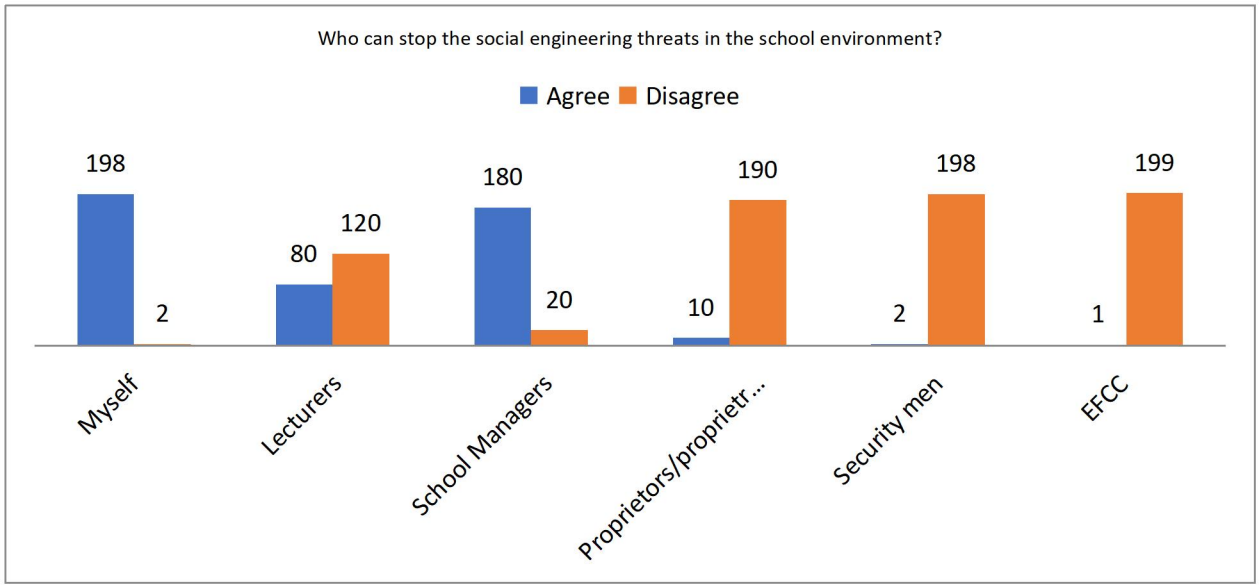


Figure 5: Chart showing who can stop social engineering attacks

A different set of private and public security agencies was put across for respondents to choose who can put stop to the attacks from social engineers. Figure-5 displayed that the attacks could be easily stopped by 'oneself' with 198 out of 200 respondents in agreement, next to this is 'school managers' with180

responses, then lecturers have 80responses while proprietor/proprietresses, security men in school, and EFCC were not significant. This implies that only oneself is the best to stop the menace.

Interview Analysis

The interviewees were asked two questions that peculiar to the study:

Do you aware that social engineers are targeting students nowadays to trap their family members?

Do you know that it is very imperative to keep your personal information safe from anybody you don't trust such as strangers, new friends etc?

Simple structured interview questions were asked with straightforward answers like 'I aware', 'I do not aware', 'I know', and 'I do not know'. The transcription was done and subjected to charts for easy interpretation and understanding.

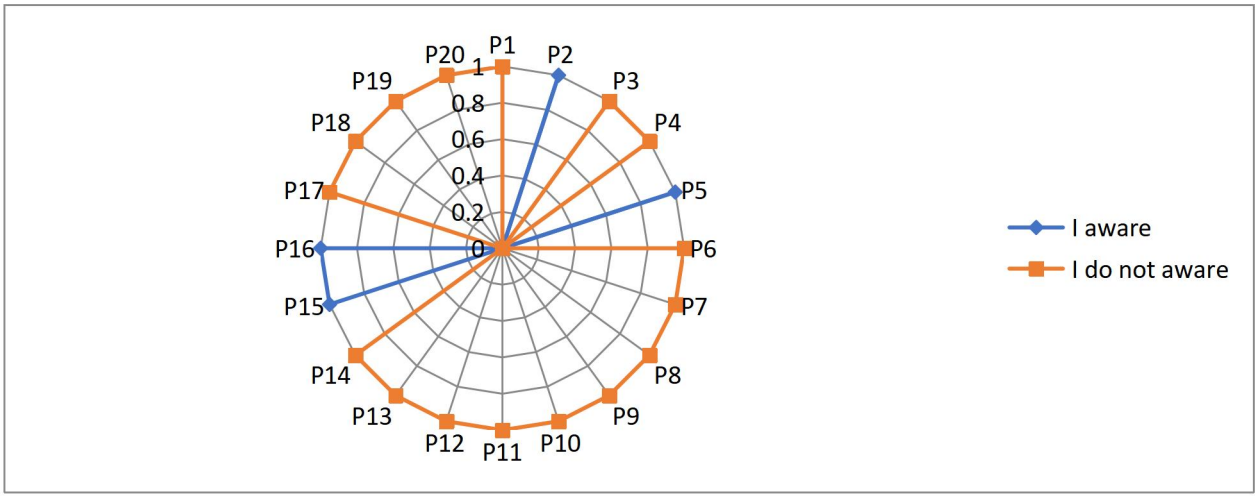


Figure 6: Showing radar chart of whether students are aware that social engineers are targeting them to trap their family members.

The chart (Radar-Figure-6) depicted that 16 participants did not aware of the social engineers' target (P1, P3, P4, P6, P7, P8, P9, P10, P11, P12, P13, P14, P17, P18, P19, and P20) while only 4 participants aware of the target (P2, P5, P15, and P16).This implies that school management must take a drastic step in making social engineering attacks open to the students repeatedly.

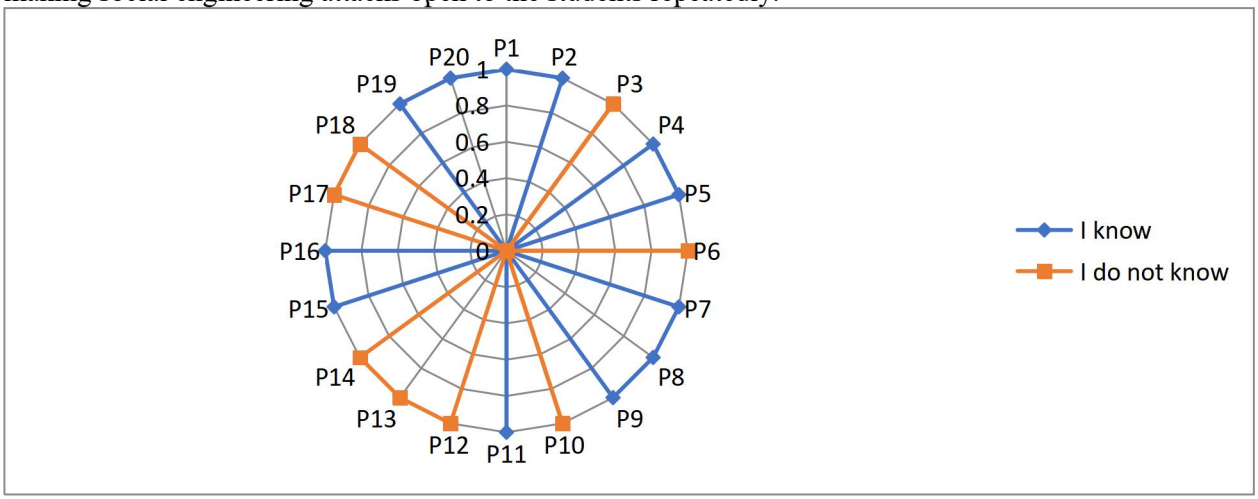


Figure 7: Showing radar chart of whether students know that it is very imperative to keep their information safe from anybody they don't trust such as strangers, new friends etc.

The chart (Radar-Figure 7) showed that only 8 participants did not know that it is very imperative to keep personal information safe from anybody we don't trust such as strangers, new friends etc (P3, P6, P10, P12, P13, P14, P17, and P18) while the remaining 12 participants know that it is very imperative to keep personal information safe from anybody we don't trust such as strangers, new friends etc (P1, P2, P4, P5, P7, P8, P9, P11, P15, P16, P19, and P20). This implies that the majority of the students know the importance of keeping personal information safe from just anybody.

Discussion

Findings clearly showed that social engineering attacks have extended to the school environment in Nigerian institutions. In this, students are their (Social engineers) main target after they have tried all means to attack their parents, families, and relatives. It was noted that the age of the students, exposure of the students to the school environment for the first time, and students' ignorance of their threats serve as prey to become their victims. Educating students about the social engineering attacks was observed very indispensable to be carried out from time to time not only during orientation periods alone. Tricks used by social engineers should be unveiled during this awareness step by step. A warning note must be sent to all students so that they can stop this danger not relying on any special forces outside the school or within the school environment. It was also noted that the majority of the student do not aware of the evils perpetrated by so-called 'social engineers' and how to keep their personal information safe from just anybody that comes their way.

Conclusion

Observation shows that higher levels of education, especially the students due to their age and exposure, are a prime target for social engineering engagement missions. According to Hasan et al (2010) user education is the first and most powerful defence against social engineering, backed up by strong, clear (written) policies that define when and to whom (if ever) users are permitted to give their passwords, open up the server room, etc. Universities, poly-techniques, and colleges worldwide house a great number of students, alumni, and staff members in their ecosystem. Efforts should be channelled towards educating all concerned individuals about the tricks and ways social engineers use to exploit information from students as a result of their ages, exposure and being a novice to the way they get close to them to steal or break through their sensitive and confidential information.

References

Ajaegbu, C; Adesegun, O. A; Adekunle, Y. A & Awodele, O (2013). *Social Engineering Attack Awareness: Case Study Of A Private University In Nigeria*. Nigeria Computer Society Conference Proceeding on e-Government

Alsulami, M.H.; Alharbi, F.D.; Almutairi, H.M.; Almutairi, B.S.; Alotaibi, M.M.; Alanzi, M.E.; Alotaibi, K.G.; Alharthi, S.S.(2021). Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia. *Information 2021, 12, 208.* https://doi.org/ 10.3390/info12050208

Arlitsch, K., & Edelman, A. (2014). Staying safe: Cyber security for people and organizations. *Journal of Library Administration*, 54(1), 46-56.

Aroyo, A.M.; Rea, F.; Sandini, G.; Sciutti, A.(2018). *Trust and social engineering in human-robot interaction: Will a robot make you disclose sensitive information, conform to its recommendations or gamble*? IEEE Robot. Autom. Lett. 2018, 3, 3701–3708.

Blancaflor, Eric & Banzon, Clarion Von Harvey (2021). *Risk Assessments of Social Engineering Attacks and Set Controls in an Online Education Environment. 3rd International Conference on Modern Educational Technology*, May 2021 Pages 69-74; https://doi.org/10.1145/3468978.3468990

Ghafir, I.; Saleem, J.; Hammoudeh, M.; Faour, H.; Prenosil, V.; Jaf, S.; Jabbar, S.; Baker, T. (2018). Security threats to critical infrastructure: *The human factor. J. Supercomput.* 2018, 74, 4986–5002.

Gioe, D. V., Goodman, M. S., & Wanless, A. (2019). Rebalancing cybersecurity imperatives: Patching the social layer. *Journal of Cyber Policy*, 4(1), 117-137.

Hasan, Mosin; Prajapati, Nilesh & Vohara, Safvan, (2010). Case Study On Social Engineering Techniques For Persuasion. *International Journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC*) 2(2), June 2010, 17-23

Kalnin, s, R.; Purin, s, J.; Alksnis, G.(2017). *Security evaluation of wireless network access points*. Appl. Comput. Syst. 2017, 21, 38–45.

Krombholz, Katharina; Hobel, Heidelinde; Huber, Markus & Weippl, Edgar (2014). *Advanced social engineering attacks*. SBA Research, Favoritenstrafe 16, AT-1040 Vienna, Austria

Maan, P. S. and Sharma, Manish (2012).Social engineering: A partial technical attack. IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, March 2012 ISSN (Online): 1694-0814 www.IJCSI.org, 557-559

McDowell, Mindi (2007). *White paper: Avoiding Social engineering and phishing attacks, cyber security Tip ST04-014*, Carnegie Mellon University, June 2007.

Nguyen, Thai H & Bhatia, Sajal (2020). *Higher education social engineering attack scenario, awareness & Training Model*. Published by DigitalCommons@SHU, 2020. Academic Festival, Event 137

Pilette, Chloe (2021). *Social engineering defined*. www.norton

Pokrovskaia, N.(2017). *Social engineering and digital technologies for the security of social capital development.* In Proceedings of the International Conference of Quality Management, Transport and Information Security, Petersburg, Russia, 24–30 September 2017; pp. 16–19.

Richardson, Michael D; Lemoine, Pamela A; Stephens, Walter E & Waller, Robert E. (2021). *Planning For Cyber Security In Schools: The Human Factor. Educational Planning* 2020 23 Vol. 27, No. 2; 23-39

Sadiku, Matthew N O; Shadare, Adebowale E & Musa, Sarhan M (2016). Social engineering: An introduction. *Journal of Scientific and Engineering Research,* 2016, 3(3):64-66.

Salahdine, Fatima & Kaabouch, Naima (2019). *Social engineering attacks: A survey. Future internet* 2019, 11, 89; doi:10.3390/fi11040089 www.mdpi.com/journal/futureinternet

Shen, L., Chen, I., & Su, A. (2017). Cybersecurity and data breaches at schools. In M. Moore (Ed). *Cybersecurity breaches and issues surrounding online threat protection* (pp. 144-174). Hershey, PA: IGI Global.

Syed, Adib Mohammed (2020). *Social engineering: Concepts, techniques and security countermeasures*.www.social engineering.com,1-5

Voxco, (2022). *Descriptive research desig*n. https://www.voxco.com

White, T L P (2015). *An Introduction to social engineering.* A Cert-Uk Publication