International Journal of Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2024.11.1

Volume 10, Issue 11
November - 2024

Social Engineering Awareness Evaluation in University of Abuja: A Pragmatic Approach

Okpanachi Ugbede Gift[1], Abiodun Esther Omolara[2], Aleshinloye Yusuf Abass[3]. and Ebelogu Christopher Ubaka[4]

Research Scholar [1] and Lecturer[2-4]

[1-4]Department of Computer Science

University of Abuja, Nigeria.

ABSTRACT

Social Engineering is one of the most significant security threats facing organizational systems and data in today's technology-saturated world. It is considered a challenge for security chains, and attacks are increasing sharply. The study aimed to assess the level of Social Engineering Awareness within the University of Abuja through a Pragmatic Approach. A total of 101 participants took part in the survey and practical experiment. Results indicated a concerning lack of awareness, with 63% of respondents having no prior knowledge of Social Engineering and its attack vectors, while only 37% demonstrated awareness. Further analysis revealed that phishing emerged as the most prevalent Social Engineering attack vector, with 50% of respondents reporting victimization. Additionally, a significant portion of participants (53%) were unaware of whether their personal computers were compromised, highlighting a lack of technological know-how and awareness as key factors contributing to vulnerability. Considering the widespread use of public computers and networks among respondents, the study underscored the high potential for successful social engineering attacks within the University community. These findings shed light on the urgent need for enhanced Social Engineering awareness and cybersecurity measures within the University of Abuja.

Keywords: Cyber security**.** Pragmatic approach, Social engineering, University of Abuja.

1.0 INTRODUCTION

Technological advancements in computing environments, including learning institutions, have led to the development of interconnected networks, uncontrolled social networking, and thousands of applications and users. These technologies are essential because they facilitate educational processes and interactions. However, the availability of such technology in advanced computing environments, particularly educational environments, opens doors for security threats by cybercriminals and hackers seeking to exploit vulnerabilities in the systems [1]. Social engineering is one of the most significant security threats facing organizational systems and data in today's technology-saturated world. It is considered a challenge for security chains, and attacks are increasing sharply [2]

Social Engineering is a collation of techniques of human manipulation by exploiting the basic emotions of human beings such as greed, distress, and naivety in order to obtain the required information [3]. In simpler words, social engineering is the method of persuading a potential victim to perform a particular action that is, sharing personal information [4]. According to Ghafir et al, [5], social engineering is defined as the art of exploiting the naivety of unsuspecting individuals and taking advantage of their weaknesses to convince them to comply with one's desires. Instead of relying on an organization's technical security shortcomings to break into its computer systems, social engineers use employees' weaknesses to mislead them into compromising the systems or turning over sensitive information.

As the use of the internet grows, social engineering is also on the rise, and the privacy of user data is being breached from time to time. Nigeria has recorded 82,000 data breaches in the first quarter of 2023 (January to March). This is according to a report by cybersecurity company Surfshark [6]. These latest numbers represent a 64% increase from the fourth quarter of 2022, in which the most populous African country recorded 50,000 data breaches. With this development, Nigeria now ranks 32nd on a list of countries with the most data breaches in the first quarter of the year 2023 this is worse than the 41st which it ranked in the last quarter of 2022. A data breach is not only a huge concern to businesses and individuals; it also comes with a great cost in terms of loss and reputational damage [7]. In recent years the world has witnessed many incidents of data and privacy breaches. In the year 2018, a British consulting firm named Cambridge Analytics got access to more than 87 million Facebook users' data and their friends' data without their user's consent [8]. According to Mumtaz [9], Facebook was fined 500,000 pounds by the UK's data protection watchdog, in October 2018. In the following year i.e., 2019, Disney+, a streaming service, was attacked and thousands of its accounts were compromised. The Washington Post reported that hackers took control of compromised accounts, changed their login credentials, and started selling them for as low as 3$ per account on the dark web [10]. In the year 2020, researchers unearth 235 million user profiles on Instagram, TikTok, and YouTube available online [11]. Also in the year 2021, IdentityForce, a U.S identity protection firm, reported more than 40 data breaches in various multinational companies around the globe [9] among several other incidences.

However, the University of Abuja, like many other educational institutions worldwide, relies heavily on digital infrastructure and information systems to support its administrative operations, academic activities, and research endeavors. While these technological advancements have undoubtedly brought numerous benefits, they have also exposed the university community to various cybersecurity risks. Among these risks, social engineering has emerged as a prominent threat that exploits human behavior and psychological manipulation to gain unauthorized access to sensitive information or compromise the university's digital assets. This research, using a pragmatic approach aims at conducting social awareness evaluation in order to improve the resilience of staff and students of the University against social engineering attack vectors.

2.0 LITERATURE REVIEW

This section focuses on recent and relevant literature relating to the study. It discusses Social Engineering and its various stages It also highlights some important research conducted in these fields of study in recent times. The research gap is also covered here

2.1 Social Engineering

According to Cindana and Ruldeviyani [12], social engineering encompasses any action aimed at influencing individuals to engage in actions that may or may not be in their best interest. This notion of social engineering is closely associated with the concept of persuasion and refers to the manipulation of people's psychology to induce them to perform activities that contravene the principles of Information Security. By employing such tactics, which rely on human interaction, criminals can potentially gain unauthorized access to sensitive data, exploiting the naivety of individuals within an organization. While social engineering is frequently utilized for malicious intentions, it can also serve as a valuable tool for identifying faults. Through its application, human errors within organizations can be detected, enabling the implementation of suitable corrective measures.

Among the several tactics employed to illicitly access information systems and acquire sensitive data, social engineering stands out as a highly resourceful method. Unlike other cybersecurity threats, this method necessitates minimal technical expertise as it predominantly exploits the human factor within an organization [1]. As integral components of computer systems, humans form an inherent part of the system's attack surface, therefore, the objective of Social Engineering (SE) attacks is to deceive individuals in order to obtain sensitive information, such as their credentials, and/or to introduce malware onto their system [13].

2.2 Stages of Social Engineering

This refers to the steps undertaken by a social engineer to effectively infiltrate their targeted organization. These steps encompass information gathering, also known as investigation, establishing a relationship, also known as a hook, exploitation, and finally, execution [14]. Figure 1 shows the various phases involved in social engineering.

DOI: 10.31695/IJASRE.2024.11.1

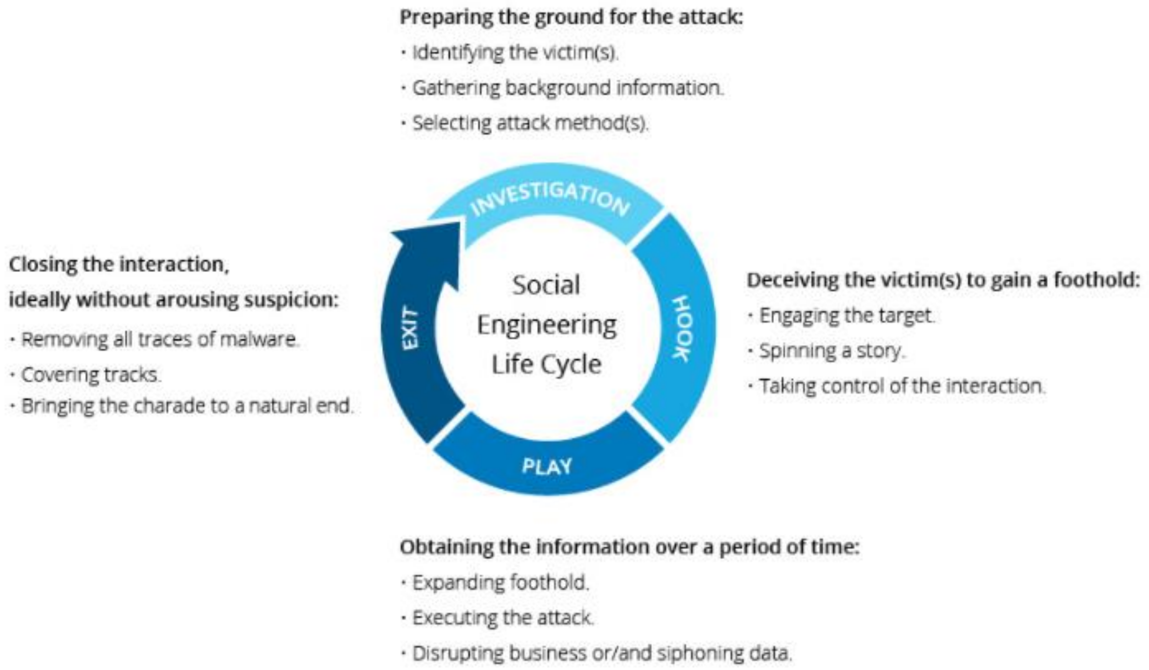

Preparing the ground for the attack:
· Identifying the victim(s).
· Gathering background information.
· Selecting attack method(s).
INVESTIGATION
HOOK
PLAY
EXIT
Social Engineering Life Cycle
Deceiving the victim(s) to gain a foothold:
· Engaging the target.
· Spinning a story.
· Taking control of the interaction.
Obtaining the information over a period of time:
· Expanding foothold.
· Executing the attack.
· Disrupting business or/and siphoning data.
Closing the interaction, ideally without arousing suspicion:
· Removing all traces of malware.
· Covering tracks.
· Bringing the charade to a natural end.

Figure 1: Social Engineering Attack Life Cycle [14].

According to Chitery and Singh [14], the motivation behind social engineering attacks can be attributed to various factors, including financial gain, access to proprietary information, competitive advantage, and even revenge or personal amusement. However, greediness remains the primary driving force behind social engineering attacks. It is noteworthy that individuals within an organization can be bribed to disclose vital and confidential information, leading to what is known as a malicious insider threat. Managing such threats is particularly challenging since both physical and login details to the organization's system are at significant risk. Common victims of social engineering attacks are often categorized as new employees, clients and customers, IT professionals, partners and contractors, top-level management, and others.

2.3 Related Works

This study explores research closely associated with social engineering attacks, which have received less attention compared to purely technical security attacks. A diverse array of research endeavors concentrates on the latter, whereas a smaller number of researchers have directed their efforts toward understanding and mitigating social engineering attacks.

Majid et al [1] conducted a study focused on assessing social engineering awareness within the Saudi educational sector. The study developed and evaluated the use of a questionnaire to measure participants' understanding of social engineering. A total of 465 respondents took part in the survey, providing insights into their knowledge of social engineering. The findings revealed that 34% of the participants (158 individuals) had prior knowledge of social engineering techniques. Moreover, the results indicated significant disparities in security practices and skills between participants with and without previous knowledge of social engineering. This study emphasizes the importance of training in enhancing awareness of social engineering attacks within the Saudi educational sector.

In their recent study, Robert and Philip [15] conducted a semi-comprehensive literature review using the PRISMA method to explore common attack methods, strategies for reducing employee susceptibility, and the importance of awareness training. The findings of the study shed light on the serious consequences of data breaches, as evidenced by notable incidents involving Yahoo and Sony. The research highlights that phishing and spear-phishing are particularly prevalent attack methods, taking advantage of human vulnerabilities and evading sophisticated security systems. To

DOI: 10.31695/IJASRE.2024.11.1

effectively mitigate risks, organizations are advised to adopt a multi-layered approach that combines technological solutions with comprehensive employee awareness training.

Elnaim et al. [16] conducted a study at Prince Sattam Bin Abdulaziz University in Saudi Arabia aimed to assess students' awareness of social engineering threats. The experimental study found that a significant majority, specifically 72% of the surveyed university students, were not familiar with the term "social engineering".

Happ et al [17] conducted an experimental study in Luxembourg to assess people's awareness of computer security. The study involved 1,208 participants who were asked about their attitudes towards computer security and their passwords. The researchers, unknown to the participants, approached them while carrying University of Luxembourg bags. The participants were divided into two groups: Group #1 and Group #2. Group #1 participants were offered chocolate before being asked for their password, while Group #2 participants received chocolate after completing the survey. The findings indicated that the provision of a small gift, such as chocolate, significantly increased the likelihood of participants divulging their passwords.

Chang and Soew [18] conducted a social engineering experiment to assess people's awareness of social engineering attacks in relation to the two-factor authentication mechanism. The results revealed that 50% of users fell victim to the attack by forwarding their authentication code to the attackers. In response to these findings, the researchers proposed a set of principles aimed at designing verification messages that are resistant to abuse, to reduce users' susceptibility to forwarding verification codes to attackers. Through the implementation of these robust messaging techniques, the success rate of such attacks was significantly reduced to only eight percent, which represents a substantial improvement compared to the standard second-factor verification code messages used by Google.

Karakasiliotis [19] adopted an experimental approach to evaluate the level of end-user awareness regarding social engineering and phishing. A web-based survey was conducted, presenting participants with a combination of 20 legitimate and illegitimate emails. These emails were categorized based on various characteristics that recipients often consider when deciding whether to trust the content or not. These characteristics included identifiable recipient, identifiable sender, images/logos, untidy layout, typos/language errors, and URL/link. The participants were required to classify the emails and provide explanations for their decisions. The findings revealed that out of the 179 participants, only 36% were successful in correctly identifying legitimate emails, while 45% were successful in spotting illegitimate ones. It was also observed that in many cases, participants who correctly identified illegitimate emails were unable to provide convincing justifications for their choices. This study emphasizes the challenges faced by end-users in effectively discerning between legitimate and illegitimate emails, as well as the potential lack of awareness regarding the reasoning behind their decisions. These findings underscore the importance of enhancing end-user education and awareness programs to mitigate the risks associated with social engineering and phishing attacks.

According to Li et al. [20], employees who are aware of their company's information security policies and procedures demonstrate higher competence in managing cybersecurity tasks compared to those who are unaware of these policies. This finding was derived from a survey conducted with 579 business managers and professionals. The researchers utilized Structural Equation Modeling (SEM) and ANOVA procedures to analyze the survey results. On the other hand, Aldawood and Skinner [21] highlighted that despite organizations having state-of-the-art cybersecurity measures and trained personnel, hackers still succeed in obtaining sensitive information. This suggests that there are persistent vulnerabilities that allow hackers to bypass security measures, despite organizations' efforts. One key concern for organizations, as noted by Siponen et al. [22], is the lack of employee compliance with information security policies (ISPs). Employees must adhere to these policies to maintain robust security. However, it is important to note that simply forcing individuals into compliance may lead to undesired behaviors or negative consequences.

Dalal and Amelia [23] conducted a study where they developed a taxonomy of defense mechanisms against social engineering. They also designed a survey to assess employee awareness of these mechanisms. Additionally, they proposed a model called Social Engineering InfoSec Policies (SE-IPs) and created a survey to measure the level of implementation of these SE-IPs. Upon analyzing the data from the first survey, the authors discovered that more than half of the employees surveyed lacked awareness regarding social engineering attacks. Furthermore, the paper

DOI: 10.31695/IJASRE.2024.11.1

examined data from a second survey, revealing that, on average, organizations incorporated slightly over fifty percent of the formal SE-IPs identified. These findings are concerning, indicating that organizations remain vulnerable to social engineering tactics.

Wenni et al. [24] employed Bryman and Bell's literature review method to conduct a systematic review of existing literature. Their research identified a novel approach, along with various methods, frameworks, models, and evaluations, for preventing social engineering attacks. Additionally, the study introduced a protocol developed by the authors themselves, which proved effective in mitigating social engineering attacks. The protocol proposed by Wenni et al. [24] encompassed strategies such as health campaigns to raise awareness, understanding the vulnerabilities of social engineering victims, and implementing a co-utile protocol that facilitates information sharing within social networks while managing associated risks. The findings of their systematic literature review offer valuable recommendations and insights into preventing social engineering attacks. This research contributes to the field by introducing new perspectives and approaches that can enhance security measures against social engineering threats.

Annarelli et al. [25] adopted a comprehensive approach that encompassed four essential components: organizational culture, employee training, incident management, and awareness-raising activities. Similarly, Aldawood and Skinner [21] emphasized the importance of providing employee awareness training.

Pavlo et al. [13] conducted a systematic review of 169 articles, examining a total of 735 hypotheses in the empirical social engineering (SE) research domain. Their study specifically focused on experimental characteristics and core cognitive features from both the attacker and target perspectives. The findings of their research indicate that previous experiments only partially replicate real-world attacks, and the scope of the exploitable SE attack surface seems to exceed the coverage provided by the existing body of research.

The study revealed that factors such as the context of the targets and their cognitive processes were frequently overlooked or not explicitly considered in the design of experimental studies. This suggests that there is room for improvement in terms of replicating real-world scenarios and considering the various contextual and cognitive elements that influence the effectiveness of social engineering attacks. The study, however, highlights the need for further research and attention to these crucial aspects in the field of social engineering.

2.4 Identified Research Gap

While social engineering awareness has been studied in various contexts, there is still a lack of research that focuses on this specific university (University of Abuja, Nigeria) and adopts a practical and real-world approach to assessing awareness levels. The absence of these studies that specifically investigate the effectiveness of pragmatic approaches (such as simulated phishing and email spoofing) for evaluating social engineering awareness within the University of Abuja exacerbates the vulnerability to social engineering attacks. Without targeted strategies and initiatives, individuals within the university community may remain uninformed and ill-prepared to recognize and mitigate social engineering threats effectively. The lack of a comprehensive and practical approach to enhancing social engineering awareness not only puts the confidentiality, integrity, and availability of human and digital assets at risk but also hinders the establishment of a proactive and security-conscious culture within the university. Therefore, this research aims to bridge this gap by identifying the prevalent social engineering attack vectors in the university, understanding the factors contributing to vulnerability, and proposing a pragmatic approach to evaluate and enhance social engineering awareness. The outcome of this research will provide insights into how the University of Abuja can proactively mitigate the risks associated with social engineering attacks and foster a security-conscious environment that empowers individuals to recognize, prevent, and respond effectively to social engineering threats.

3.0 RESEARCH METHODOLOGY

In this section, the research design, methodologies, participant selection (population), instruments, and data collection procedure are thoroughly examined and justified. Additionally, an explanation is provided regarding the data processing methods employed. The section also includes a discussion of the experimental procedures.

3.1 Research Design

This research inquiry adopts a quantitative approach, using survey and practical experimental methods, it focuses majorly on phishing and email spoofing of social engineering vectors and employs a study design that offers a cost-effective means of gathering information from the target population, which consists of University of Abuja staff and students. The methodology and research activities are divided into two phases as follows:

3.1.1 Phase 1: Survey method

The survey method was employed to provide qualitative insights into participant's understanding of social engineering risks and their level of confidence in identifying and responding to attacks.

3.1.2 Phase 2: Simulated Email Spoofing and Phishing Attack

Conducting simulated email spoofing and phishing attacks can gauge how well the staff and students of the University of Abuja can identify and respond to deceptive emails, messages, or phishing URLs. The metrics that were considered include the overall click rate on malicious links, susceptibility to providing sensitive information, and the ability to report suspicious attempts.

The tools that were used for this process are:

i. Django Python framework
ii. MySQL Database system.
iii. Deceptive domain name and URL

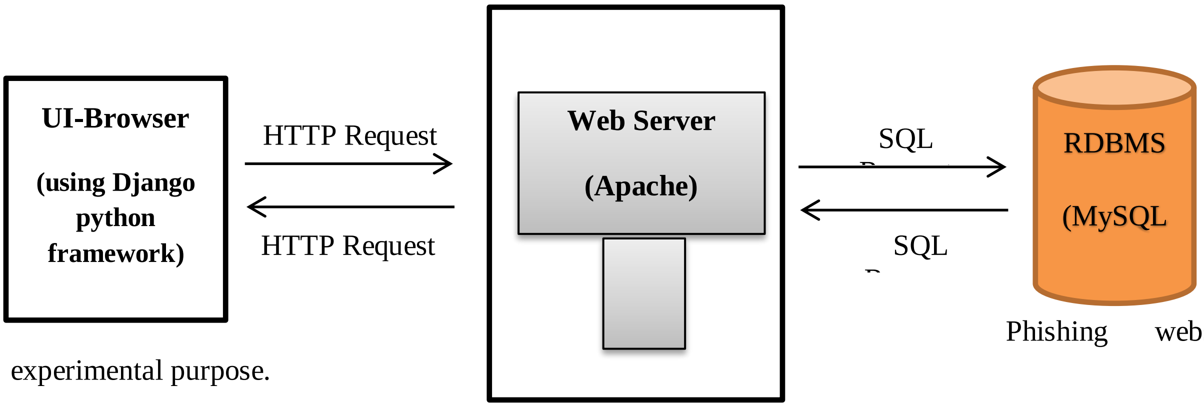


Figure 3.1: Architecture of the Simulated Phishing website for the experimental purpose.

The activities under this phase include:

i. A cloned University of Abuja and Facebook website were developed to look exactly like legitimate websites.
ii. Email addresses of participants were collected via Google Forms while answering the survey questions.
iii. Deceptive links of the cloned websites were forwarded to participants' email addresses collected using email spoofing. This enabled the researcher to evaluate the overall click rate on malicious links, susceptibility to providing sensitive information, and the ability to report suspicious attempts.

3.2 Sources of Data

The study utilizes data sourced directly from a primary source, specifically in its raw form using Google form and practical experimental setups in order to assess the level of social engineering awareness at the University of Abuja.

3.3 Method of Data Collection

While various primary methods of data collection exist, including surveys, questionnaires, interviews, and experiments, this study specifically utilized a self-administered questionnaire via Google Form and conducted practical experiments to gather quantitative data from the University of Abuja community. This method was chosen due to the limited time available for data collection processes.

3.4 Sampling Process

This study employed convenience sampling as the sampling method, which falls under non-probability sampling. Convenience samples are selected based primarily on their proximity to the researcher, making them quick and easy to gather without the need for additional selection criteria. The participation of the target population, consisting of university staff and students, in this survey study varied based on their availability and willingness to respond and participate in the practical experiment. The survey questions were constructed by combining nominal and interval scales. The nominal scale questions included both open-ended and closed-ended (multiple choice) formats, both of which were utilized in this study. To enhance the number of responses, the survey was distributed using a social distribution method, leveraging social media platforms.

3.5 Data Analysis Method

The responses from the Google Form were exported in the Google sheet file format (CSV). The datasets were then cleaned and prepared for analysis. To analyze the data and create visual representations, tables, and charts were generated. Microsoft Excel software pivot table and Statistical Package for the Social Sciences (SPSS) were utilized by the researchers to cross-tabulate the data and generate visualizations for analysis purposes.

3.6 Data Presentation

The analyzed data from the study were visually presented in figures, utilizing charts. The presentation of the data in figures includes the use of frequency distribution tables, which conveniently group the data. Column charts were consistently employed in this research to enhance memory retention and facilitate comprehension of the analysis.

4. RESULTS AND DISCUSSION

4.1 RESULTS

The results of the survey and practical experiments are discussed in this section. It presents an in-depth analysis that sheds light on the research problems addressed in this paper. The goal of this study is to evaluate the level of Social Engineering awareness at the University of Abuja using a Pragmatic Approach. The outcomes of the analysis in this section were directed by the research questions and interpreted using the collected primary data [10].

4.2 Demographics

The characteristics of the population being examined to observe behavior or trends for knowledge discovery are described by the demographics. The age, gender, and educational background of the participants are all disclosed in this study. The distribution of the demographics is in the following sub-sections.

4.2.1 Age Distribution

Table 4.1 and Figure 4.1 shows the age distribution of respondents used in the study

Table 4.1: Age of Respondents

S/N	Age Bracket	Frequency	Percentage	Cumulative Percentage
1	0 - 17	9	9%	9%
2	18 - 39	37	36%	45%
3	40 - 65	27	27%	72%
4	66 - Older	28	28%	100%
	Total	101	100%	

DOI: 10.31695/IJASRE.2024.11.1

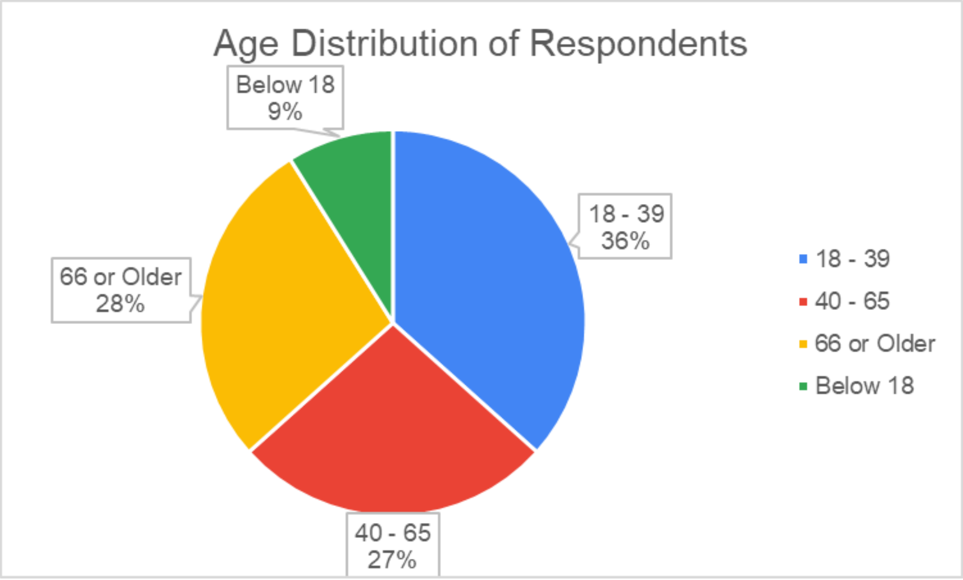


Figure 4.1: Age Distribution of Respondents

Table 4.1 and Figure 4.1 showed that out of the 101 respondents, 9% of the participants were below 18 years of age, 36% were between 18 and 39, 27% were between 40 to 65, and 28% were aged 66 and above.

4.2.2 Gender Distribution of Respondents

Table 4.2 and Figure 2 shows the gender distribution of respondents used in the study.

Table 2: Gender of Respondents

S/N	Gender	Frequency	Percentage	Cumulative Percentage
1	Female	65	64%	64%
2	Male	36	36%	100%
	Total	101	100%	

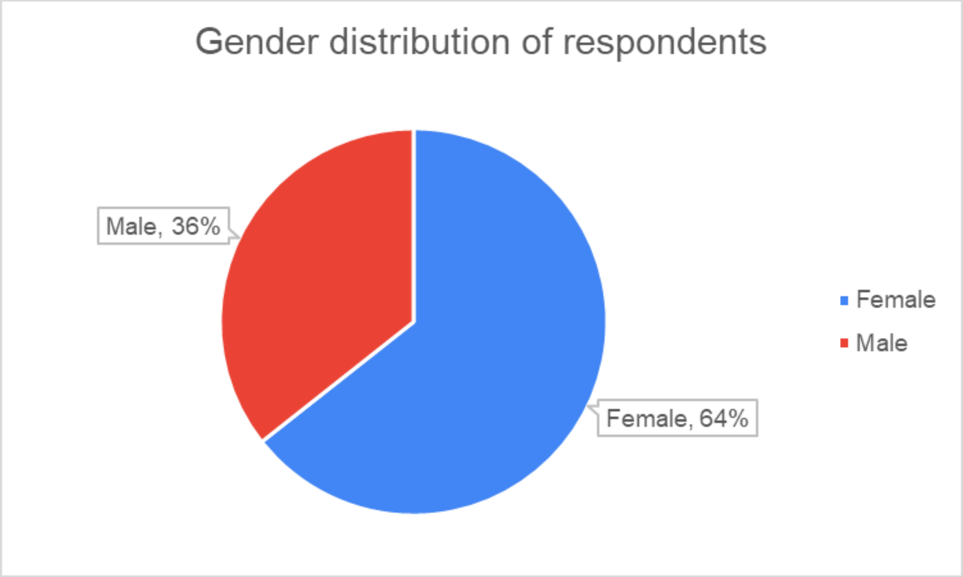


Figure 3: Age Distribution of Respondents

Table 3 and Figure 4.2 show that 64% of the participants who took part in the survey were female, while the remaining 36% of the participants were male.

DOI: 10.31695/IJASRE.2024.11.1

4.2.3 Educational Background of Respondents

Table 4.3 and Figure 4.3 shows the highest educational qualifications distribution of respondents used in the study.

Table 4.3: Educational qualification of respondents

S/N	Level of Education	Frequency	Percentage	Cumulative Percentage
1	MSc/PhD	46	45%	45%
2	BSc/HND	37	37%	82%
3	ND/NCE	0	0%	82%
4	Olevel/FSLC	18	18%	100%
	Total	101	100%	

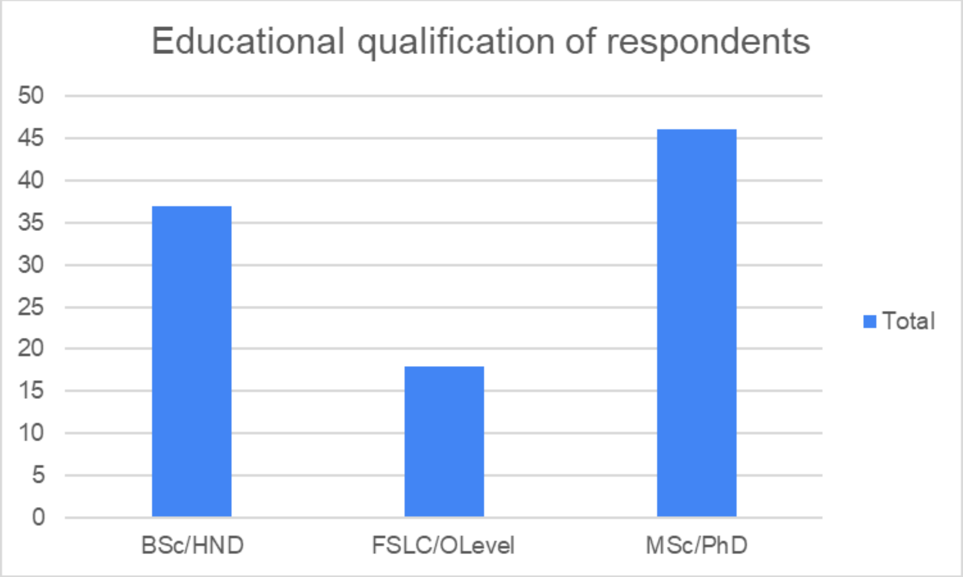


Figure 4: Educational Qualification of Respondents

From Table 4.3 and Figure 4, it was observed that out of the 101 respondents, 46 respondents representing 45% already bagged an MSc or PhD, 37 representing 37% have got BSc or HND, 18 representing 18% have got O'level or FSLC.

4.3 Data Analysis and Presentation

The subsequent section further analyses the data obtained from the respondents of the questionnaire in relation to the theme: Understanding social engineering and having knowledge of information security, Practices related to securing information and ensuring its confidentiality, integrity, and availability, Technological measures implemented to enhance security and protect against potential threat. The presentation is however done to provide answers to all the outlined research questions.

4.3.1 Understanding Social Engineering and Having Knowledge of Information Security

Table 4.4, Figure 4.5, Figure 4.4, and Figure 4.5 shows the number of respondents who have had prior knowledge of Social Engineering and its attack vectors.

Table 4.4: Respondent's prior knowledge of SE and its attack vectors.

S/N	Prior Knowledge of SE	Frequency	Percentage	Cumulative Percentage
1	No	64	63%	63%
2	Yes	37	37%	100%
	Total	101	100%	

DOI: 10.31695/IJASRE.2024.11.1

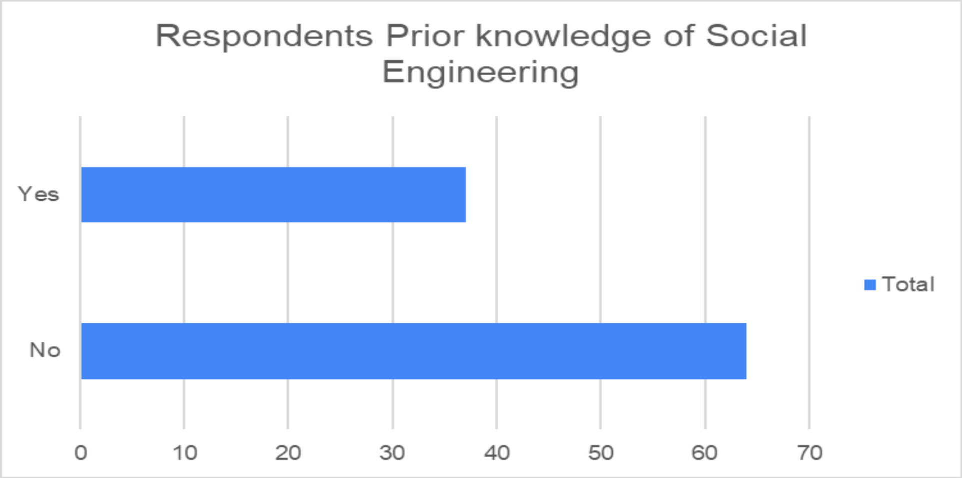


Figure 5 Respondent's Prior Knowledge of SE and its Attack Vectors.

From Table 4.4 and Figure 5 above, it is evident that out of 101 respondents, 64 representing 63% have no prior knowledge of Social Engineering and its attack vectors, and only 37 representing 37% are aware of Social Engineering and its attack vectors. This shows a very low awareness level which further provides an answer to **Research Question I** of this study.

4.3.2 Social Engineering Attack Vectors

Table 4.5 and Figure 4.5 shows the various Social Engineering attack vectors respondents have been victims of.

Table 4.5: SE attack vectors respondents have been victims of.

S/N	**SE attack vectors respondents have been victims of.**	**Frequency**	**Percentage**	**Cumulative Percentage**
1	Phishing	50	50%	50%
2	Pretexting	9	9%	59%
3	Email Spoofing	29	28%	87%
4	Cannot Say	13	13%	100%
	Total	101	100%	

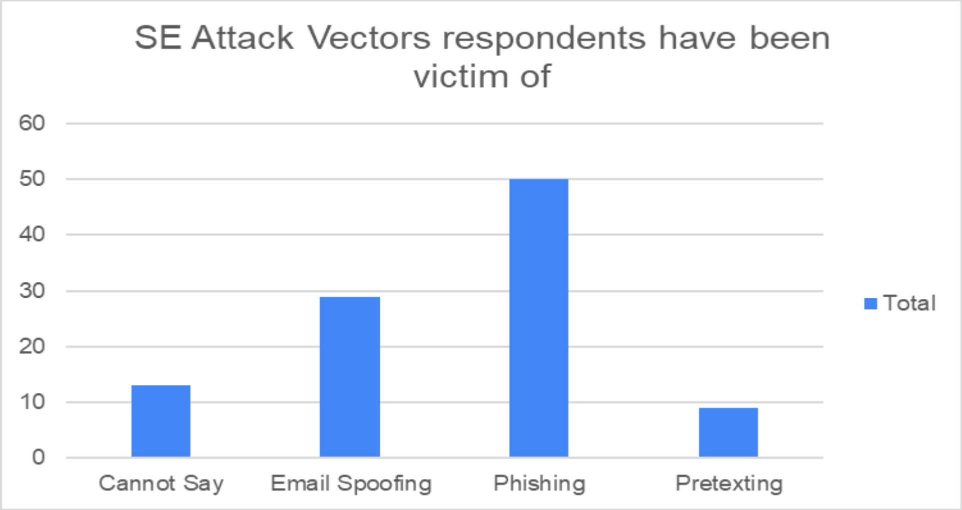


Figure 6: SE Attack Vectors Respondents have been Victims of.

DOI: 10.31695/IJASRE.2024.11.1

From Table 4.5 and Figure 6, it is evident that out of 101 respondents, 9 representing 9% were able to identify that they have once, twice, or more been victims of pretexting, 29 representing 28% stated they have been victims of email spoofing, 13 representing 13% could not even identify the social engineering they have been victim of, 50 representing 50% stated they have been victim of phishing. This finding however revealed Phishing as the most prevalent Social Engineering attack vector in the University of Abuja community, which further provides answers to **Research question II** of this study.

4.3.3 Factors Responsible for Social Engineering Vulnerability

Table 4.6 and Figure 4.6 reveal the factors responsible for Social Engineering vulnerability in the University of Abuja community.

Table 4.6 Factors responsible for SE vulnerability in University of Abuja community.

S/N	Factor responsible for SE vulnerability	Frequency	Percentage	Cumulative Percentage
1	No	54	53%	53%
2	Yes	47	47%	100%
	Total	101	100%	

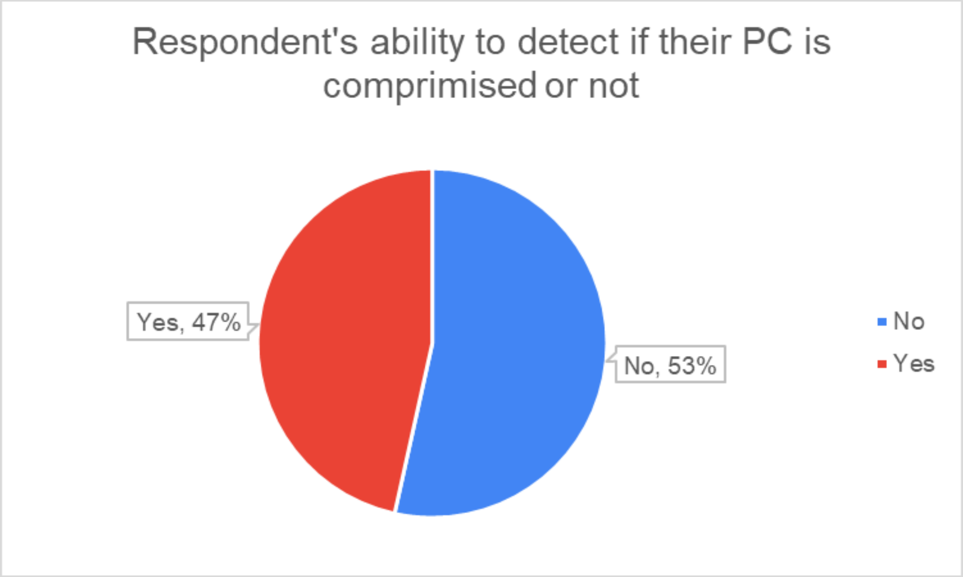


Figure 7: Factors Responsible for SE Vulnerability

From Table 4.6 and Figure 4.6, it is evident that out of 101 respondents, 54 representing 53% have no idea if their personal computer (PC) is compromised or not. Only 47 representing 47% could identify if their PC was compromised by hackers or social engineers. This finding reveals a lack of technological know-how and lack of Social Engineering awareness as major factors responsible for Social Engineering vulnerability in the University of Abuja community which further provides an answer to **Research question III** of this study.

4.3.4 Possibilities of Successful Social Engineering Attack in the University Community

Table 4.7 and Figure 4.7 reveal the possibilities of a successful Social Engineering attack within the University of Abuja community.

DOI: 10.31695/IJASRE.2024.11.1

Table 4.7 Respondents that have used a public pc or network to access their private information

S/N	Factor responsible for SE vulnerability	Frequency	Percentage	Cumulative Percentage
1	Yes	101	100%	100%
2	No	0	0%	100%
	Total	101	100%	

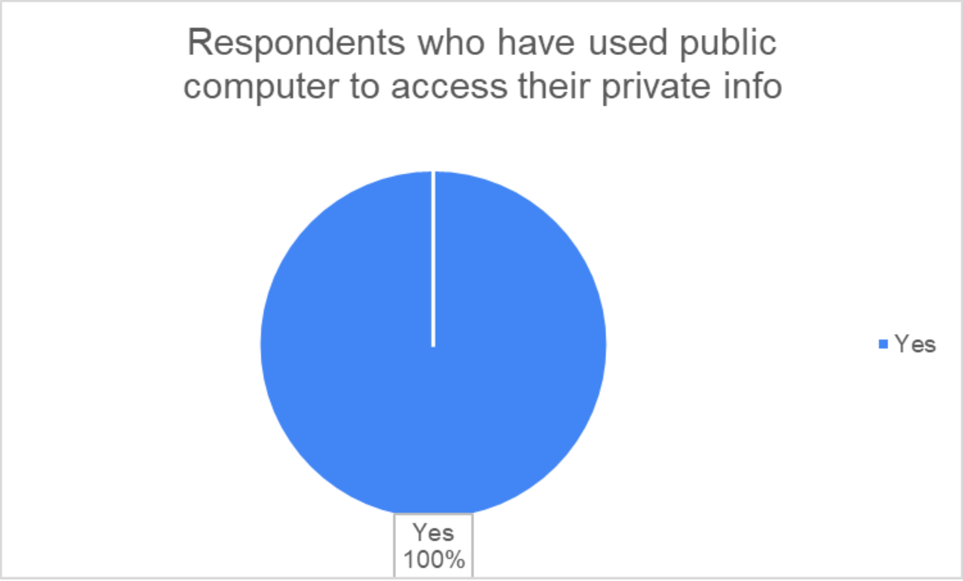


Figure 4.7: Respondents that have used a Public PC or Network to Access their Private Information

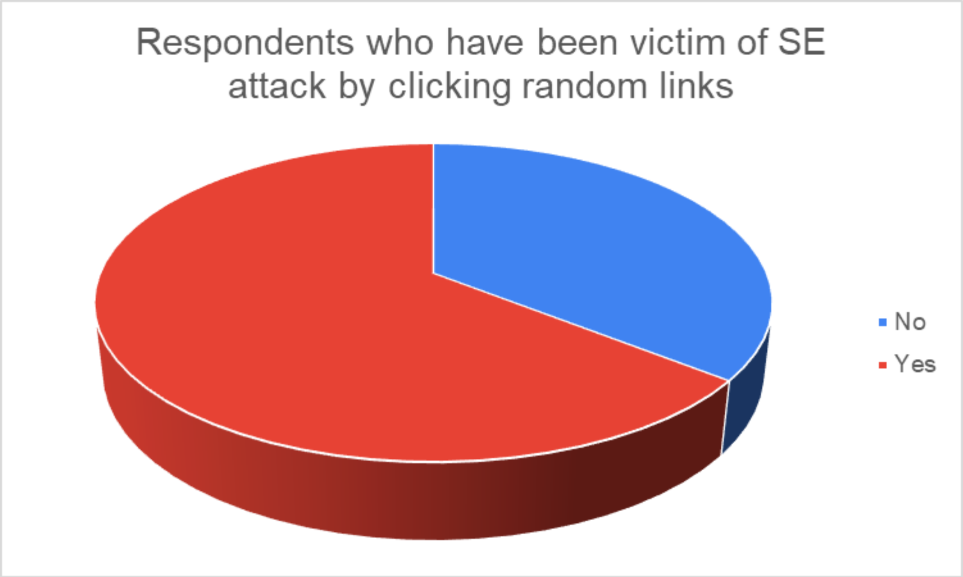
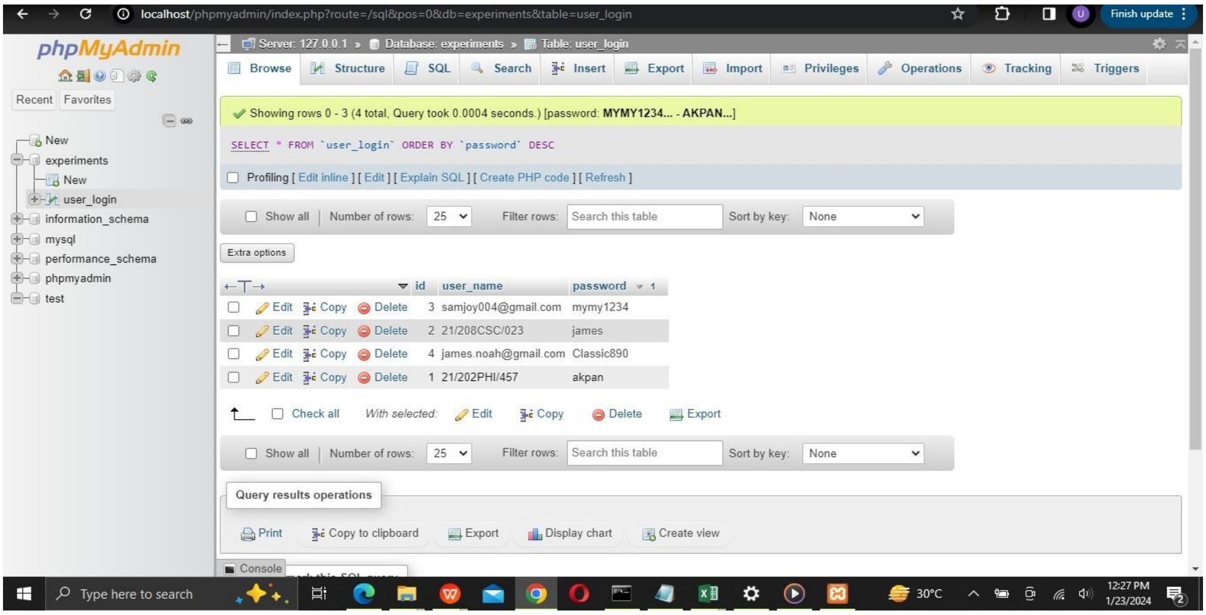


Figure 4.8: No of Respondents who have been Victims of SE Attack by Clicking Random Links.

DOI: 10.31695/IJASRE.2024.11.1



localhost/phpmyadmin/index.php?route=/sql&pos=0&db=experiments&table=user_login

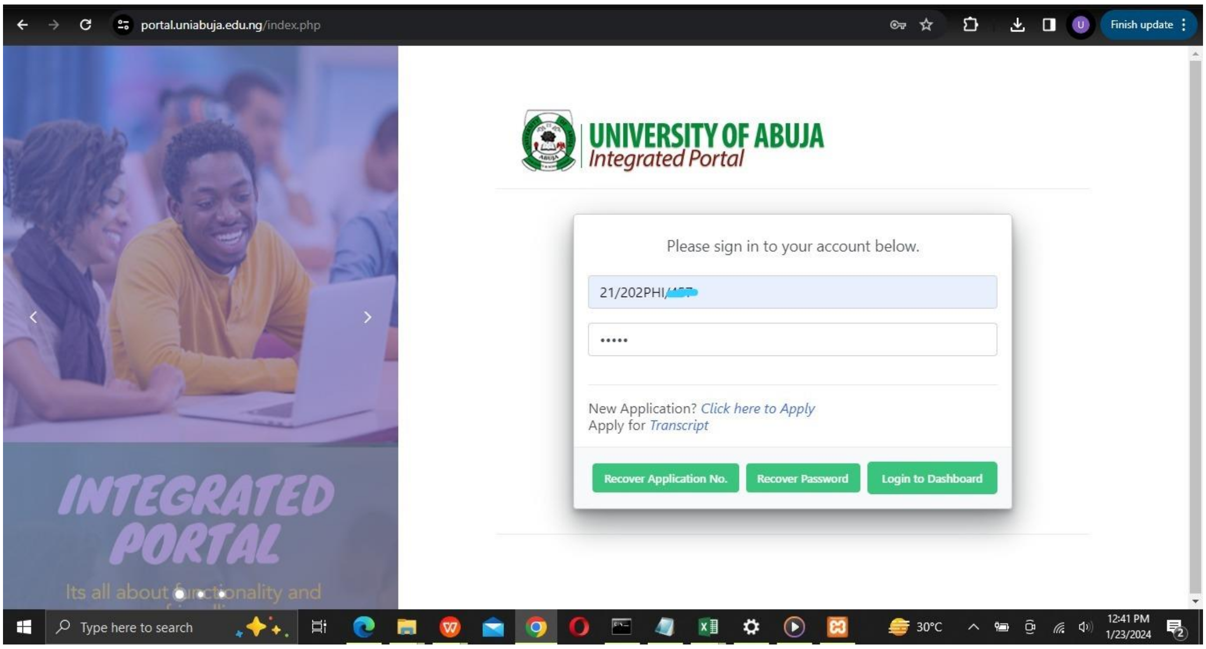
Server: 127.0.0.1 » Database: experiments » Table: user_login

✓ Showing rows 0 - 3 (4 total, Query took 0.0004 seconds.) [password: **MYMY1234... - AKPAN...**]

```
SELECT * FROM `user_login` ORDER BY `password` DESC
```

id	user_name	password
3	samjoy004@gmail.com	mymy1234
2	21/208CSC/023	james
4	james.noah@gmail.com	Classic890
1	21/202PHI/457	akpan

Figure 4.9: Some Acquired info from the Experiment' Portal Backend



portal.uniabuja.edu.ng/index.php

UNIVERSITY OF ABUJA
Integrated Portal

Please sign in to your account below.

21/202PHI/[redacted]

•••••

New Application? *Click here to Apply*
Apply for *Transcript*

Figure 4.11: Respondents Supplying their Login Details to a Cloned UofA Website.

Recall that from Table 4.4 and Figure 4.4, it is evident that out of 101 respondents, 64 representing 63% have no prior knowledge of Social Engineering and its attack vectors, and only 37 representing 37% are aware of Social Engineering and its attack vectors. This shows a very low awareness level which further provides an answer to research question I of this study. Also, from Table 4.7 and Figure 4.7 a total of 101 of the respondents, representing 100% use public computers or networks to login or access their personal information. Figure 4.9, Figure 4.10, and Figure 4.11 also show respondents supplying their login details to cloned websites. With the low Social Engineering awareness level and this attitude of using public PC or networks to access their personal information and with unsuspecting respondents supplying their login details to cloned websites, the possibility of a successful social engineering attack in the University community is high. These, however, provide answers to **Research Question IV** of this study.

DOI: 10.31695/IJASRE.2024.11.1

5.0 CONCLUSION

This research has revealed critical aspects of Social Engineering Awareness within the University of Abuja community, employing a pragmatic approach. The study revealed a concerning lack of awareness among respondents, with a majority having no prior knowledge of Social Engineering and its attack vectors. The prevalence of phishing as the most significant attack vector underscores the urgency of tailored educational initiatives. Moreover, the identified lack of technological know-how emphasizes the need for not only awareness programs but also technical literacy efforts to empower individuals in recognizing and mitigating Social Engineering threats. The research findings also highlight a potentially high risk of successful attacks in shared computing environments, necessitating enhanced security measures. The recommendations for educational initiatives, targeted phishing mitigation strategies, technical literacy programs, and improved security for public computers provide a roadmap for addressing these vulnerabilities. As the University of Abuja community moves forward, it is imperative to prioritize and implement these recommendations to fortify its resilience against Social Engineering threats and foster a culture of cybersecurity awareness and competence.

REFERENCES

[1] Majid H., Fawaz D., Hamdan M., Bandar S., Mohammed M., Majdi E., Khaled G. and Sultan S. (2021) Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia. Information, 2021.

[2] Salahdine, F. and Kaabouch, N. (2019) Social Engineering Attacks: A Survey., vol. 89, Future Internet, 2019, p. 11.

[3] Mumtaz H. (2022) "Social Engineering and Data Privacy, [Online]. Available: https://www.researchgate.net/publication/367484714. [Accessed 3rd June 2023].

[4] Leonov, P. Y., Vorobyev, A. V., Ezhova, A. A., Kotelyanets, O. S., Zavalishina, A. K., and Morozov, N. V. (2021) "The Main Social Engineering Techniques Aimed at Hacking Information Systems," in *Ural Symposium on Biomedical Engineering, Radioelectron*, 2021.

[5] Ghafir I. Saleem J., Hammoudeh M., Faour H., Prenosil V., Jaf S., Jabbar S. and Baker T., (2018) Security threats to critical infrastructure: The human factor.," *J. Supercomputer,* p. 74, 2018.

[6] Surfshark (2023) "Data breach statistics 2023’Q1 vs. 2022’Q4," [Online]. Available: https://surfshark.com/research/study/data-breach-statistics-2023-q1. [Accessed 3rd June 2023].

[7] Aridor G., Che Y., and Salz T. (2020) "The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR," *SSRN Electronic Journal,* p. doi:10.2139/ssrn.3522845, 2020.

[8] Isaak J. and Hanna M., (2018) "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection," *Computer,* p. 56–59, 2018.

[9] Mumtaz H., Samrina S. and Noman I. (2023) "Social Engineering and Data Privacy.," Research Gate, 2023.

[10] Telford, T. (2019) "Thousands of Disney Plus accounts were hacked and sold online for as little as $3.," 2019. [Online].

[11] Bischoff, P. (2020) "Social media data broker exposes nearly 235 million profiles scraped from Instagram, TikTok, and YouTube. ComparìTech. A Global Perspective," 2020, p. 18 (1) 40–46.

[12] Cindana A. and Ruldeviyani Y. (2018) "Measuring Information Security Awareness on Employee Using HAIS-Q: Case Study at XYZ Firm," in *International Conference on Advanced Computer Science and Information*

DOI: 10.31695/IJASRE.2024.11.1

Systems (ICACSIS), Yogyakarta, Indonesia, 2018.

[13] Pavlo B., Luca A., and Nicola Z. (2022) Cognition in Social Engineering Empirical Research: a Systematic Literature Review, ACM Comput. Surv, 2022.

[14] Chitrey, A., Singh, D., & Singh, V. (2012) A comprehensive study of social engineering based attacks in india to develop a conceptual model, *International Journal of Information and Network Security*, vol. 1, no. 2, p. 45, 2012.

[15] Robert B. and Philip S. (2023) The Human Element of Cybersecurity: A Literature Review of Social Engineering Attacks and Countermeasures., DiVA. Dalarna University, Dalarna, 2023.

[16] Elnaim B, H. and Al-Lami H. (2017) The current state of phishing attacks against Saudi Arabia University students., *International Journal of Computer Applications Technology and Research*, vol. 6, no. 1, pp. 42-50, 2017.

[17] Happ C., Melzer A., and Steffgen G. (2016) Trick with treat–reciprocity increases the willingness to communicate personal data., in *Computers in Human Behaviour*, 2016, p. 372–377.

[18] Chang K.C., and Seow Y.M. (2014) Effects of it-culture conflict and user dissatisfaction on information security policy non-compliance: A sense-making perspective., in *A Global Perspective 18*, 2014, p. 40–46.

[19] Karakasiliotis A., Furnell S., and Papadaki M. (2016) Assessing end-user awareness of social engineering and phishing,. Decision Support Systems," in *Decision Support Systems*, DSS, 2016, p. 154–165.

[20] Li L., He W., Xu L., Ash I., Anwar M., and Yuan X. (2019) Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior, *International Journal of Information Management*, vol. 45, no. 1, p. 13–24., 2019.

[21] Aldawood H. and Skinner G. (2019) Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues, in *Future Internet*, 2019, p. 73.

[22] Siponen M., Mahmood M.A., and Pahnila S. (2014) Employees' adherence to information security policies: An exploratory field study. in *Information and Management*, 2014, p. 217–224..

[23] Dalal A. and Amelia R. (2021) A Literature Survey and Analysis on Social Engineering Defense Mechanisms and Infosec Policies. *International Journal of Network Security and Its Applications (IJNSA)*, vol. 13, no. 2, 2021.

[24] Wenni S., Zarina S., Umi-Asma M, Rossilawati S., and Muhammad A. (2022), Social Engineering Attacks Prevention: A Systematic Literature Review., IEEE Access., 2022.

[25] Annarelli, A., Nonino, F., and Palombi, G. (2020) Understanding the management of cyber resilient systems.," Computers and Industrial Engineering, 2020.

[26] Taherdoost, H. (2021) Data Collection Methods and Tools for Research; A Step-by-Step Guide to Choose Data Collection Technique for Academic and Business Research Projects. *International Journal of Academic Research in Management (IJARM)*, vol. 10, no. 1, pp. 10-38, 2021.

Corresponding Email: ugbede.okpanachi2020@uniabuja.edu.ng