WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

User Behavior Towards Social Engineering Attacks, Risk Factors Associated and Security Awareness on Some Selected Users of Mobile Devices of Kebbi State Polytechnic Dakingari

Shamsu Sani[1], Anas Shehu[2], Atiku Abubakar[3], Sufiyanu Muhammad[4]

Department of Computer Science Kebbi State Polytechnic dakingari[1,2]
Department of Computing Science, School of Natural and Computing Science, University of Aberdeen, Aberdeen- United Kingdom [3]
Department of Mathematics Kebbi State Polytechnic dakingari[4]

ABSTRACT

Social engineering attempts have made cyberspace extremely vulnerable to security breaches. However, much remains unknown about the nature and mechanics of social engineering attacks. Understanding user behavior, identifying associated risk factors, and improving security awareness are critical to protecting personal and institutional information in light of the proliferation of mobile devices and the sophistication of cyber threats. This study looks into the social engineering attack behavior patterns of a particular user group at Kebbi State Polytechnic Dakingari. Through the use of an extensive survey methodology, the study pinpoints common risk factors such as a lack of awareness, insufficient cyber security training, and an excessive dependence on default security settings. The study also evaluates the participants' current security awareness, highlighting areas that need more education and highlighting the urgent need for customized cyber security awareness programs in the academic community. Based on the research outcomes, recommendations are made for the creation of customized security training modules, the use of multifactor authentication, and the encouragement of a cyber security-conscious culture. By improving user knowledge, developing critical thinking abilities, and encouraging a proactive security mindset. This study advocates for a comprehensive strategy to reduce social engineering risks and strengthen mobile device users' defense against cyber threats, resulting in a safer digital environment.

Keyword: Social Engineering Attack, Cyber security, awareness, Risk factor

I. INTRODUCTION

Mobile devices are now essential instruments in our daily lives in a time of fast technological advancement. They allow for easy communication, convenient transactions, and instant access to information by seamlessly connecting us to the digital world. But this unprecedented reliance on mobile devices has also made consumers more vulnerable to various cybersecurity threats. Of these, social engineering attempts are one of the most prevalent and sneaky problems that both individuals and businesses must deal with. Social engineering attacks, such as Phishing, use psychological tricks to trick users into disclosing private information, giving bad actors access to private information without authorization. These attacks can have disastrous repercussions, including compromised digital security, identity theft, and financial losses.

These risks also affect mobile device users at educational institutions like Kebbi State Polytechnic Dakingari. Developing successful cybersecurity tactics requires a thorough understanding of user behavior in response to social engineering attacks, as well as the identification of risk factors and the degree of security awareness of these users. This study explores how users behave in complex ways when confronted with social engineering attacks at Kebbi State Polytechnic Dakingari. This study attempts to identify the trends and driving forces behind a particular user group's reactions to social engineering techniques.

Additionally, it seeks to identify the specific risk factors that render these users susceptible to such assaults. Additionally, the study evaluates the users' current security awareness, revealing information on their familiarity with cybersecurity best practices and their capacity to spot and foil social engineering scams.

This study seeks to inform policymakers, educators, and security experts in addition to offering significant insights into the topic of cybersecurity through a thorough investigation of user behavior, risk factors, and security awareness. Through comprehension of the subtleties of social engineering assaults and the elements impacting user susceptibility, interested parties can create focused instructional initiatives, put strong security protocols in place, and cultivate a mindset of alertness and adaptability to these constantly changing digital hazards.

such assaults. Additionally, the study evaluates the users' current security awareness, revealing information on their familiarity with cybersecurity best practices and their capacity to spot and foil social engineering scams.

This study seeks to inform policymakers, educators, and security experts in addition to offering significant insights into the topic of cybersecurity through a thorough investigation of user behavior, risk factors, and security awareness. Through comprehension of the subtleties of social engineering assaults and the elements impacting user susceptibility, interested parties can create focused instructional initiatives, put strong security protocols in place, and cultivate a mindset of alertness and adaptability to these constantly changing digital hazards.

Using psychological traits of people to break into a computer system is known as social engineering, or SE. Usually, this is done by tricking a person into doing things like installing software. The skill of tricking users into compromising information systems is known as social engineering. Within the domain of computer and cyber security, social engineering designates a form of assault wherein the assailant leverages human weaknesses through strategies like coercion, influence, fraud, manipulation, and incitement in order to obtain classified data, breach security objectives (like confidentiality, integrity, availability, controllability, and auditability) of cyberspace elements (like infrastructure, data, resource, user, and operation), or gain unauthorized access to restricted areas.

In a nutshell, social engineering is a kind of attack where the attacker takes advantage of social interaction and human frailty to get past cyberspace security measures. Social engineers use influence and persuasion to manipulate people with access to information, either into disclosing sensitive information or even into carrying out their harmful attacks, as opposed to using technological means to attack systems. Usually, technical defenses against this form of attack are ineffectual. (Syed, n.d.).

In the context of cyber security, social engineering is defined as one of the illicit acts carried out by cybercriminals that involves psychological manipulation to deceive innocent parties into giving up sensitive personal information or data to the attacker. Instead of threatening the victim, the attacker usually uses persuasion and building trust. The social engineer exploits the victim's mistake, which places the victim in danger. Instead of breaking into the software, the cybercriminal employs social engineering techniques since it is much simpler to trick the victim into providing sensitive information to the attacker than it is to crack the victim's password and obtain information the hard way (Luo et al., 2011).The sensitive information can be bank account numbers, passport information, credit and debit card numbers and other data that is confidential and crucial (Syed, n.d.).

More often than not, social engineering techniques will be used as an attack vector by an adversary than any other sophisticated technological exploit. Thus, social engineering attacks represent a serious risk to society's security. Attacks using social engineering are not just targeted at PC users. Mobile device users have been the victim of a sharp rise in Social Engineering assaults over the last five years, most of which take use of human factor flaws. Since social engineering is the most common method of malware distribution on mobile platforms, attacks targeting mobile users through social engineering have grown to be a serious problem for both individuals and companies.

Since the 1970s, social engineering has become a fairly common attack among the hacker community. In contrast to traditional computer attacks, which involve using software vulnerabilities and brute-force password cracking, social engineering attacks concentrate on using human vulnerabilities to get around security barriers and get past firewalls and antivirus software without the need for deep coding. Attacks using social engineering can be expensive for institutions and organizations. 32% of all businesses worldwide, regardless of size, and 48% of major businesses had experienced 25 or more social engineering attacks in the last two years.

. Thirty percent of large companies indicated that social engineering attacks can cost more than 100,000 USD per instance. In 2018, 85% of organizations were attacked, an increase by 16%, and the average annual cost reached 1.4 million USD [6]. A study conducted by (cite here) indicated that the FBI's data gives an average cost of 130,000 USD and that costs can extend to millions of dollars in some cases (Alsulami et al., 2021).

Therefore, the contribution of this paper is a method of measuring behavior, awareness and risk factor associated in social engineering attacks of mobile device users in kebbi state Polytechnic Dakingari Community, through the use of a questionnaire. The study addresses the main factors that can increase the awareness of social engineering in the community. This paper is structured as follows: Section 2 reviews the literature; Section 3 explains the problem statement; Section 4 presents the research methodology; Section 5 discusses the results; Section 6 identifies the limitation; and Section 7 provides a conclusion and recommendations for future work

II. LITERATURE REVIEW

(Ahmed et al., 2018) investigated how Social Engineering (SoE) affects risk factors in institutions of higher learning. Additionally, look into how personal productivity is affected when Social Engineering (SoE) attacks occur in higher education institutions due to threats, vulnerabilities, and digital evidence of information security attacks. It suggests that the effects of social engineering (SoE) attacks have a major influence on individual productivity in higher education institutions. It was discovered that, should this type of attack occur, the impact would be moderate.

(Alsulami et al., 2021), In order to give a measurement of social engineering awareness, the study examined the Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia. findings show that, in terms of their security practices and abilities, those who had previously learned about social engineering differed significantly from those who had not. The study suggests that raising awareness of social engineering attacks in the Saudi educational sector requires training.

(Heartfield & Loukas, 2015), investigated Attacks by Social Engineering: A The frequency and intensity of social engineering and survey attacks have been rising, and they are harming individuals and businesses financially and emotionally. Novel detection and countermeasure strategies are therefore

desperately needed, as are employee and K–12 student training programs. An extensive overview of social engineering assaults, including their categories, detection techniques, and preventative measures, is provided by Countries.

(Wang et al., 2021) examined social engineering in cybersecurity, focusing on attack methods, human vulnerabilities, and effect mechanisms. The study produced a conceptual model that offers a structural and integrative viewpoint for explaining the operation of social engineering attacks. with knowledge of the mechanisms underlying social engineering attacks. where more than 40 human vulnerabilities and more than 30 effect mechanisms are compiled. And provide examples of how to apply these principles, weaknesses, and attack techniques to comprehend the operation and impact of social engineering attacks.

Human weaknesses that have been described include gullibility, avarice, ignorance, curiosity, carelessness, and helpfulness. However, merely focusing on human weaknesses is insufficient to explain the mechanisms underlying social engineering attempts. Some works addressed or included the effect mechanism in various contexts.

(Ferreira et al., 2015) Analyzed the relationship (equal, include, overlap) between the aforementioned principles and presented a combined list of social engineering persuasion principles: i) authority; ii) social proof; iii) liking, similarity & deception; iv) commitment, reciprocation & consistency; and v) distraction. However, these works did not pay close attention to human weaknesses, nor do they address other facets of effect mechanisms.

(Bitton et al., 2020) A framework for assessing smart phone users' information security awareness (ISA) for particular attack classes is presented in the study, which examined the information security awareness of 162 users over the course of a long-term user survey. Research indicates that there is a large discrepancy between users' self-reported and real activity, and that users' capacity to mitigate SE attacks is strongly connected with the ISA level obtained from their actual conduct.

III. PROBLEMSTATEMENT

Social engineering assaults continue to be a problem, especially for mobile device users, even with the quick development of cyber security defenses. This study attempts to look into how chosen mobile device users at Kebbi State Polytechnic Dakingari behave when faced with social engineering attacks. The study will investigate the risk factors that are intrinsic to these attacks, evaluate the targeted users' security awareness, and pinpoint the knowledge and practice gaps that leave them open to these kinds of cyber threats. The value of the data contained in information systems has expanded along with its use in many different types of institutions. E-learning, student registration, and other systems are only a few of the uses for which numerous educational institutions have created E-Systems. Particularly during the COVID-19 pandemic, when online interaction was the primary means of communication with students, the significance of these technologies has been noted. Because of their significance, educational institutions became the target of numerous cyber security assaults. For instance, Information 2021, 12, 208 6 of 13 ransom ware attacked the University of Calgary, and in order to prevent any data loss, they had to pay 20,000 CAD.

IV. SOCIAL ENGINEERING ATTACKS CURRENTLY

The largest threat to Cyber Security at the moment is social engineering. The authors of claim that although they can be identified, they cannot be stopped. Social engineers prey on victims in order to obtain private information that may be sold on the dark web and black market or utilized for particular reasons. Since the emergence of big data, attackers have used it to their advantage to profit from important data for companies. They compile enormous volumes of data into items that are sold in large quantities in today's markets.

Although social engineering attacks differ from each other, they have a common pattern with similar phases. The common pattern involves four phases: (1) collect information about the target; (2) develop relationship with the target; (3) exploit the available information and execute the attack; and (4) exit with no traces.

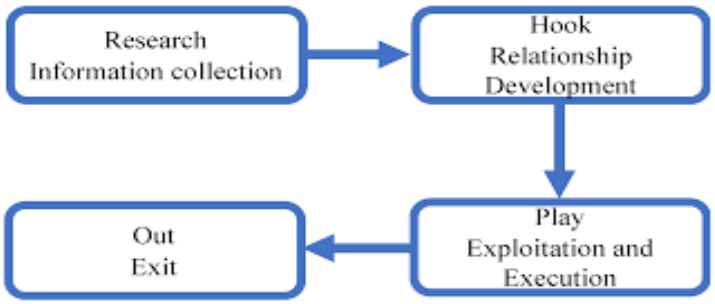

Figure 1: Social Engineering Attack Stages

The attacker chooses a victim based on a set of criteria during the research phase, which is also known as information gathering. Using email or direct contact, the attacker begins to win the victim's trust during the hook phase. During the pay phase, the attacker uses emotional blackmail to coerce the

victim into disclosing personal information or making security blunders. The attacker leaves during the out phase without leaving any evidence. (Salahdine & Kaabouch, 2019).

Attacks Classification

Social engineering attacks can be classified into two categories: human-based or computer-based

Figure 2: Social Engineering Attack Classification

When conducting a human-based attack, the attacker interacts with the victim directly in order to obtain the necessary information. They can therefore only affect a certain number of victims. To obtain information from the targets, software-based attacks are carried out utilizing gadgets like computers or mobile phones. They can attack a large number of targets quickly. Spear phishing emails involve computer-based attacks, one of which is the social engineering toolkit (SET). Based on how they are carried out, social engineering assaults may also be divided into three categories: physical, technological, and societal attacks. As shown in the figure below

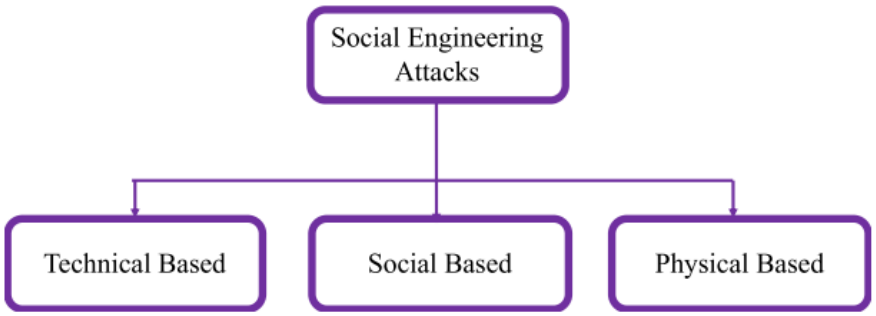

Figure 3: Social Engineering Attack Classification

Attacks based on social psychology manipulate victims' emotions and psychology through ties with them. The fact that these attacks entail human contact makes them the most successful and hazardous. Spear phishing and baiting are two examples of these assaults. Technical attacks obtain required data, including passwords, credit card numbers, and security questions, by using the internet to access social networks and websites of online businesses. Attackers who use physical means to gather information about their target are said to be conducting physical-based attacks. Dumpster diving for important papers is one example of such an attack. As previously said, social engineering attacks can incorporate human, computer, technical, sociological, and physical elements. Examples of social engineering attacks include phishing, impersonation on help desk calls, shoulder surfing, dumpster diving, stealing important documents, diversion theft, fake software, baiting, quid pro quo, pretexting, tailgating, Pop-Up windows (Salahdine & Kaabouch, 2019).

Various viewpoints allow for the classification of social engineering attacks into multiple categories. They can be divided into two groups based on the type of entity involved: software or humans. In addition, they can be divided into three groups based on the manner in which the attack is carried out: physical, technical, and social attacks. We are able to categorize social engineering attacks into two primary groups by examining the various classifications that are currently in use: direct and indirect. Attacks falling under the first category are carried out through direct communication between the attacker and the target. They speak of assaults carried out by touch, gaze, or vocal communication. In order to carry out the attack, they might also demand that the attacker be present in the victim's working space. Examples of these attacks are: physical access, shoulder surfing, dumpster diving, phone social engineering, pretexting, impersonation on help desk calls, and stealing important documents. Attacks classified under the indirect category do not require the presence of the attacker to launch an attack. the attack can be launched remotely via malware software carried by email's attachments or SMS messages. Examples of these attacks are: phishing, fake software, Pop- Up windows, ransom ware, SMS phishing, online social engineering, and reverse social engineering.

V. Attacks Description

A Phishing Attacks:

The most frequent type of assault carried out by social engineers is phishing. Through phone calls or emails, they attempt to deceitfully get private and personal information from their intended targets. Attackers deceive victims into divulging private and sensitive information. Phishing websites, emails, advertisements, scareware, antivirus software, PayPal websites, prizes, and freebies are all involved. An example of an attack could include receiving a call or email from a fictitious lottery department claiming to be the winner of a large quantity of money and asking for personal information, or it could involve clicking on a link that is attached to the emails. These details could include the person's mother's name, birthplace, visited places, credit card information, insurance information, complete name, physical address, pet name, first or ideal career, and any other information useful to access private accounts, like internet banking, or services. Phishing attacks can be classified into five categories: spear phishing, whaling phishing, vishing phishing, interactive voice response phishing, and business email compromise phishing as illustrated in Figure 4 below:

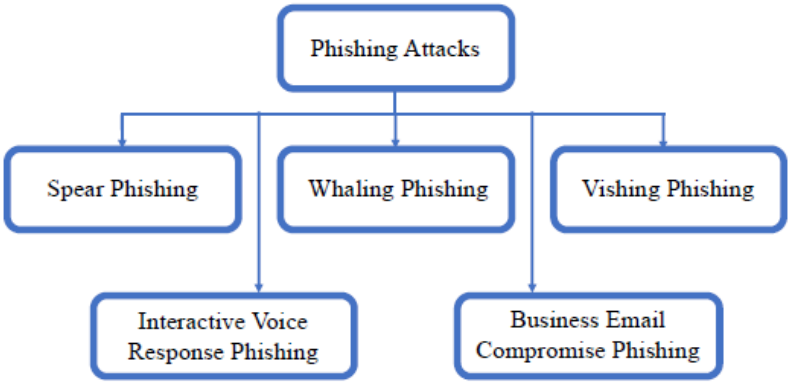

Figure 4: Phishing Attacks

Spear phishing assaults are specialized forms of phishing that use the names of particular people or groups to make statements or send messages. They necessitate gathering victim information via readily available internet data. Because these attacks come from within, it is challenging to identify and differentiate them from authentic users, which accounts for their high success rate when compared to other forms of social engineering attacks. A spear phishing attack known as "whaling phishing" targets high-profile employees of businesses called "big fishes." Vishing assaults are phone phishing schemes used to trick people into providing sensitive information for validation, such as when a bank calls. The term "vishing" refers to this type of assault, which is carried out over voice over the internet protocol (VoIP). It is a combination of the words "voice" and "phishing." Using an interactive voice response system to trick the target into entering personal information as though it comes from a reliable source is known as interactive voice response phishing.

Spear phishing assaults are specialized forms of phishing that use the names of particular people or groups to make statements or send messages. They necessitate gathering victim information via readily available internet data. Comparing these attacks to other forms of social engineering, their high success rate can be attributed to the difficulty in identifying and differentiating them from genuine users because they target an entity from within. A spear phishing attack known as "whaling phishing" targets high-profile employees of businesses called "big fishes." Vishing assaults are phone phishing schemes used to trick people into providing sensitive information for validation, such as when a bank calls. This assault is known as "vishing," which is a combination of the words "voice" and "phishing," and it is carried out over voice over the internet protocol (VoIP). The technique of interactive voice response phishing involves tricking the target into entering personal information by pretending it is from a reputable company or financial institution.

B. Pretexting Attacks

The goal of pretexting attacks is to obtain a victim's personal information by creating fictitious but plausible scenarios. They are predicated on fabrications meant to engender victim belief and trust in the assailant. The attack is carried out by text messages, phone calls, or physical media. To carry out their attack, attackers disclose information in phone books, open websites, or conferences attended by colleagues in the same field. A friend's request for access to something, an offer to provide a service or obtain employment, an inquiry about personal information, or winning the lottery could all serve as pretexts.

C. Baiting Attacks

Phishing attempts that entice users to click on a link in order to receive free items are known as baiting assaults, also referred to as road apples. They function similarly to trojan horses in that the assault is carried out by taking advantage of unprotected computer resources such storage media or USB drives that are infected with malware and are discovered by victims in a coffee shop. The USB drive behaves like a real-world trojan horse and attacks the PC when the victims plug it into their machines. Without the victims seeing, this attack carries out harmful deeds in the background. The authors detailed the use of a trojan horse-like baiting attack called Controller Area Network (CANDY) in the entertainment system of automobiles. By

interfering with the communication between the driver and the car, this assault affects the security features of the vehicle. It's done by recording the driver's speech, which enables the attacker to get inside the victim's car through the rear entrance, gather information on how the vehicle is driven, and take control of the vehicle.

D. Tailgating Attacks

In order to gain access to unauthorized buildings, tailgating attacks—also known as piggybacking or physical access—involve following an individual with security clearance into an area or building. As an example, an attacker may ask a victim to hold a door open because they have forgotten their company ID card or RFID (radio-frequency identification) card. They may also take advantage of a victim's computer or smartphone to carry out malicious activities, such as installing malware software. One of the most common ways that attackers gain access to restricted areas for malicious purposes is by using RFID cards (Salahdine & Kaabouch, 2019).

RFID systems are the newest and most widely used technology that businesses are using to manage access to their facilities because of its affordability and widespread use. Despite their benefits, they have flaws that might be used against them to provide businesses major security problems. There are multiple layers in the interconnection system model (ISO) where RFID assaults can be conducted. For example, the physical interface and RFID devices are the targets of an RFID communication manipulation at the physical layer. The RFID cards may sustain temporary or permanent damage as a result of these attacks. The RFID network is manipulated by the attacker at the network layer level, including data exchange and communication between RFID units.

E. Ransomware Attacks

Another hazard that targets people and businesses is ransomware. The FBI recently revealed that losses resulting from ransomware assaults in 2016 were around $1 billion, demonstrating the significant financial harm that ransomware can inflict upon businesses. A ransomware attack's aftereffects may cost more money than the ransom itself. Companies who are impacted by ransomware attacks may experience years of suffering as a result of lost revenue, clients, information, and productivity. By encrypting the victim's files and data, ransomware attacks limit and prevent access to them. The victim is threatened with publication of these files unless they pay a ransom to retrieve them.. Bitcoins, an untraceable, uncontrolled digital money, are required to be used for this payment. A ransomware assault can be examined using either static or dynamic analysis. Highly qualified engineers and experts in programming languages carry out static analysis by creating programs to study and comprehend the attack in order to neutralize it or recover the encrypted contents. The process of dynamic analysis involves watching the malware's operations from a distance. To run untrusted programs without causing damage to the systems, trusted systems must be used.

A Ransomware attack involves six stages: (1) creating the malware; (2) deployment; (3) installation; (4) command and control; (5) destruction; and (6) extortion

VI. RESEARCH METHODOLOGY

In order to identify the level of awareness of Social engineering attacks in the Kebbi state polytechnic Dakingari, this study started with a literature review, followed by a quantitative Survey. The literature review findings were utilized to develop the questionnaire items. The items were then grouped into four categories (i.e., knowledge, practices, solutions, and education) to reflect various level of awareness. A questionnaire was developed by the authors and then reviewed by a group of experts in the computer science department of Kebbi state polytechnic Dakingari. After passing the content validity phase, the questionnaire was created through Google forms and the link to questionnaire is https://docs.google.com/forms/d/e/1FAIpQLSckRu1E8BX0i0Fzq2lOOQTXIy3daPcAYGFSIs-a6vzqCCly-Q/viewform?usp=sf_link . A pilot phase was conducted with a group of participants to identify any spilling or timing issues. The researchers obtained ethical approval for this research from the Research Ethics Committee at Kebbi state polytechnic Dakingari. The population of the study consisted of students, teaching staff and non-teaching staff in Kebbi state polytechnic Dakingari. The link to the questionnaire was sent to participants through email and the researchers applied sampling techniques to collect more responses. The questionnaire consists of 27 questions and is divided into three parts. The first part acts as a cover letter and a consent form for the questionnaire by providing information about the study and the research team. The second part collects the respondent's demographic data including age, nationality, educational background, and gender. The third part contains statements designed to measure the awareness level of social engineering attacks in the Kebbi state polytechnic Dakingari. The fourth part allows the respondents to add any comments regarding the study.

Data Analysis

A total of 511 respondents, These respondent are Students, Teaching staff and Non-Teaching staff of Kebbi State Polytechnic Dakingari, which have responded to the questionnaire. The analysis was conducted using the statistical package for the social sciences in

IBM SPSS version 27.

VII. RESULT

TABLE I

DEMOGRAPHIC INFORMATION OF STUDENTS

Variables	Characteristics	Frequency (%)
Gender	Male	243(73.9)
	Female	86(26.1)
Age	18-24	289(87.8)
	25-34	40(12.2)
	35 above	0
Total		329(100%)

This part presents the results of collected data from students, teaching staff and non-teaching staff of Kebbi state polytechnic Dakingari, which have responded to the questionnaire. The collected data has been analyzed using Frequency and Percentage. This section presents the demographic results, the perspective of SEA (Social Engineering Attacks) responses, and other factors contributing to the cyber security knowledge of participants, which are illustrated in both (Frequency and Percentage) in the following tables. Table I demonstrates the demographic data of students, and the total number of responded students N = 329, of which 243(73.9%) of them were male, 86(26.1%) were female. Students' age is shown in three age groups; the data illustrates that the participating students in this research were mostly aged 18-24 years old 289(87.8%). Also, 40(12.2%) were aged between 24-34 years old, and 0(0.0%) were aged 35 years old and above.

TABLE II

DEMOGRAPHIC INFORMATION OF TEACHING STAFF

Variables	Characteristics	Frequency (%)
Gender	Male	89(86.4)
	Female	14(13.6)
Age	25-34	34(33.0)
	35-44	57(55.3)
	45 above	12(11.7)
Educational level	B.Sc.	27(26.2)
	M.Sc.	69(67.0)
	PhD	7(6.8)
Total N (%)		103(100%)

Table II illustrates the information on the demographic of teaching staff in this study. The data shows that the responded staff N = 103, where the majority of them were male 89(86.4%), while 14 of them (13.6%) were female. The data presents that the staff ranged in age from 25 to 45 years old (and above), with the largest portion of staff being aged between 35-44 years old 57(55.3%). Also, 34(33.0%) were aged between 25-34 years old, and just 12(11.7%) were aged 45 years old and above. The other demographic question was related to education levels. There were three education levels of teaching staff; the education level started from the lowest education level (B.Sc.) and was rated as a minimum 27(26.2%), to the highest education level (Ph.D.) with a rate 7(6.8%). In addition, the data present that those who have (M.Sc.) were rated as a maximum rate of education level 69(67.0%).

TABLE III

DEMOGRAPHIC INFORMATION OF NON - TEACHING STAFF

Variables	Characteristics	Frequency (%)
Gender	Male	54(68.4)
	Female	25(31.6)
Age	18-24	13(16.5)
	25-34	26(32.9)
	35-44	29(36.7)
	45 above	11(13.9)
Educational level	SSCE	7(8.9)
	ND/NCE	12(15.2)
	HND	16(20.2)
	B.Sc.	35(44.3)
	M.Sc.	7(8.9)
	PhD	2(2.5)
Total N (%)		79(100%)

Table III illustrates the information on the demographic of non-teaching staff in this study. The data shows that the responded staff N = 79, majority of them were male 54(68.4%), while 25 of them representing (31.6%) were female. The data presents that the age of non-teaching staff ranged from 18 to 45 years old (and above), with the largest portion of staff being aged between 35-44 years old 29(36.7%). Also, 13(16.5%), 26(32.9%) and 11(13.9%) were aged between 18-24, 25-34 years old and 11(13.9%) were aged 45 years old and above. The other demographic question was related to education

levels. There were five education levels for non-teaching staff; the education level started from the lowest education level (S.S.C.E.) and was rated as a minimum 7(8.9%), to the highest education level (Ph.D.) with a rate 2(2.5%). In addition, the data present that those who have (an M.Sc.) were rated as a maximum rate of education level 69(67.0%).

TABLE IV

CYBER-SECURITY AWARENESS AND SOCIAL ENGINEERING ATTACKS FOR ALL PARTICIPANTS

Variables	Characteristics	All participants by Frequency (%)
Which type of device do you use?	Smart phone	488(95.5)
	Tablet	7(1.4)
	Laptop/Desktop	16(3.1)
	Other	0(0)
Which Operating System do you use on your Device?	Android	475(93.0)
	iOS(iPhone/iPod)	18(3.5)
	Windows	16(3.1)
	Linux	2(0.4)
Are you previously Familiar with the term Social Engineering Attack?	Yes	187(36.6)
	No	324(63.4)
Have you ever received suspicious emails, messages, or calls asking for personal information?	Yes	387 (75.7)
	No	124(24.3)
If yes, did you recognize them as social engineering attempts?	Yes	259 (66.9)
	No	128(33.1)
If yes, how did you respond?	Provide the information	11 (4.2)
	Ignored/deleted	241 (93.1)
	Reported to authority	7(2.7)
Do you use strong, unique passwords for your online accounts (including email, social media, and banking)?	Always	210(41.1)
	Sometimes	151(29.5)
	Rarely	85(16.6)
	Never	65(12.8)
Have you ever shared your passwords or PINs with anyone?	Yes	63(12.3)
	No	448(87.7)
Do you regularly update your device's operating system and applications to the latest versions?	Yes	78(15.3)
	No	443(86.7)
Do you use security features such as biometric authentication (fingerprint, face recognition) on your device?	Yes	487(95.3)
	No	24(4.7)
Have any of your device or account (email, WhatsApp, etc) been previously Compromised	Yes	49(9.6)
	No	397(77.7)
	Not sure	65(12.7)
What information do you think social engineering attackers might target from you?	Personal details	109(21.3)
	Financial information	241(47.2)
	Social media login credentials	108(21.1)
	Work related information	53(10.4)
In your opinion, what factors increase the risk of falling victim to social engineering attacks?	Lack of awareness about SEA	314(61.4)
	Trusting unknown source or links	77(15.1)
	Weak password	56(11.0)
	Lack of security software on device	43(8.4)
	Lack of regular software update	21(4.1)
Have you received any cyber security or social engineering awareness training at Your Institutions?	Yes	0(0)
	No	511(100)
Total N (%)		511(100%)

This study has also investigated and examined the participants' further knowledge to determine whether they have sufficient information about Social Engineering awareness or whether they have been targeted by Social Engineering attacks. Although in this section, all participants (both students and staff) were asked the same questions, thus we present all participants together as presented in (Table IV).

All participants' Cyber security awareness and Social Engineering attacks are shown in Table IV, to emphasize and highlight the general behavior of all participants in these areas. According to our findings, 488(95.5%) of all participants devices were Smart phones. However, 7(1.4%) and 16(3.1%) of

participants used “Tablet” and “Laptop/Desktop” as their devices respectively. Also, 475(93.0%) participants uses Android as their Operating System, 18(3.5%), 16(3.1%) and 2(0.4%) participants uses iOS(iPhone/iPod), Windows and Linux respectively as their Operating System.

Majority of responses have shown that they are not previously Familiar with the term Social Engineering Attack with 324(63.4%). Only187(36.6%) responses are previously Familiar with the term Social Engineering Attack, this indicates that the participants have significantly awareness of cyber-security about their valuable data being targeted by hackers, and they have a high level of SE awareness to safeguard their private data.

The data also presents that 387 (75.7%) participants have previously received suspicious emails, messages, or calls asking for personal information, only 124(24.3%) participants have not previously received suspicious emails, messages, or calls asking for personal information. Out of 387(75.7%) participants that have previously received suspicious emails, messages, or calls asking for personal information, 259(66.9%) participants recognize them as social engineering attempts while 128(33.1%) participants did not recognize them as social engineering attempts. Majority of the participants that have previously received suspicious emails, messages, or calls asking for personal information, 241 (93.1%) Ignored or deleted the request that received while 11 (4.2%) provided their information and 7(2.7%) reported to the authority. However, only 210(41.1%) of respondents, were using the same password for multiple accounts on social media. Hence, this would assist hackers to access multiple accounts for each user. This will significantly increase the chance of attackers using a brute-force attack to access accounts based on the trial-and-error method.

Interestingly, the majority of responses have shown that they have not ever shared their passwords or PINs with anyone. Specifically, 448(87.7%).Only 63(12.3%) shared their passwords or PINs with someone, this will significantly allowed the attackers easily to access your accounts. Moreover, the responses have shown that majority of the participants 443(86.7%) do not regularly update their device's operating system and applications to the latest versions, only 78(15.3%) participants do regularly update their device's operating system and applications to the latest versions. 487(95.3%) participants use security features such as biometric authentication (fingerprint, face recognition) on their devices, while only few responses 24(4.7%) do not use security features such as biometric authentication (fingerprint, face recognition) on their devices.

Our finding shows that 49(9.6%) participants device or account (email, WhatsApp, etc) have been previously Compromised while the majority of the participants 397(77.7%) device or account (email, WhatsApp, etc) have never been Compromised. Also, 314(61.4%) responses have the opinion that lack of awareness about SEA is one of the major factor for falling victim to social engineering attacks while 77(15.1%), 56(11.0%), 43(8.4%), and 21(4.1%) participants responses have the opinion that Trusting unknown source or links, Weak password, Lack of security software on device and Lack of regular software update about SEA is one of the major factor for falling victim to social engineering attacks.

Finally, the results demonstrated that participants’ awareness of Social Engineering Attacks and knowledge of cyber-security attacks are limited, as they would not be able to prevent themselves from Social Engineering Attacks and cyber-security attacks without receiving an up to date training in this area.

VIII. Conclusions

The frequency of social engineering attacks has increased recently, and with it has come an increase in the damage these attacks cause, impacting both individuals and organizations in different ways. As one of the primary causes of social engineering attacks is thought to be human error, there is a need to raise awareness of social engineering tactics and the methods employed in these attacks. Due to the fact that educational institutions serve a diverse range of users, including staff, students, and people of all ages, they are susceptible to numerous social engineering attacks. This study attempted to determine the present levels of knowledge about social engineering techniques among Kebbi State Polytechnic Dakingari's students, faculty, and non-teaching staff. Members who have previously encountered social engineering techniques have superior information security practices, knowledge, and abilities, according to the study's results. This demonstrates how crucial it is to be informed about and receive educational training in social engineering methods and information security procedures. It is also clear from the results that different age and work groups use technological security solutions differently. Based on this, educational institutions must create customized training programs that take into account the unique needs of each category, including age, occupation, and educational attainment. Future work could entail creating a training curriculum that meets the specific requirements of various employee categories while increasing awareness of social engineering techniques.

REFERENCES

Ahmed, S., Khidzir, N. Z., & ... (2018). Towards The Impact of Social Engineering (SoE) Attacking Risk Factors in Higher Learning Institute. Journal of Engineering …, 3, 1–5. http://jetonline.bmi.unikl.edu.my/docs/vol6-1-5.pdf

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 saudiarabia. Information (Switzerland), 12(5), 1–13. https://doi.org/10.3390/info12050208

Bitton, R., Boymgold, K., Puzis, R., & Shabtai, A. (2020). Evaluating the Information Security Awareness of Smartphone Users. Conference on Human Factors in Computing Systems - Proceedings. https://doi.org/10.1145/3313831.3376385

Ferreira, A., Coventry, L., &Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9190(May 2017), 36–47. https://doi.org/10.1007/978-3-319-20376-8_4

Heartfield, R., & Loukas, G. (2015). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. ACM Computing Surveys, 48(3). https://doi.org/10.1145/2835375

Luo, X., Brody, R., Seazzu, A., &Burd, S. (2011). Social engineering: The neglected human factor for information security management. Information Resources Management Journal, 24(3), 1–8. https://doi.org/10.4018/irmj.2011070101

Salahdine, F., &Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4). https://doi.org/10.3390/FI11040089

Syed, A. M. (n.d.). Social engineering: Concepts, Techniques and Security Countermeasures.

Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. IEEE Access, 9, 11895–11910. https://doi.org/10.1109/ACCESS.2021.3051633