International Journal of Research Publication and Reviews

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

Assessing the Vulnerability and Impact of Social Engineering Attacks on Mobile Users in Edo State

Engr. Clement Agbeboaye[1] and Engr. Emmanuel Omosigho[2]

[1,2]Department of Electrical/Electronic Engineering Technology, National Institute of Construction Technology and Management, Uromi, Edo State, Nigeria.

ABSTRACT

Social engineering attacks pose significant cybersecurity threats by exploiting human psychology rather than technical vulnerabilities. This study assessed the vulnerability and impact of social engineering attacks on mobile users in Edo State, Nigeria. A structured questionnaire was used to collect data from 267 respondents across three locations—Benin City, Uromi, and Ewohimi—representing urban, semi-urban, and rural settings. The study employed a stratified random sampling technique to ensure broad demographic representation. Descriptive statistics and multiple regression analysis were used to evaluate respondents' awareness levels, security practices, and experiences with social engineering attacks. The results revealed that despite high awareness levels, many users lacked effective security practices, making them susceptible to attacks such as phishing, vishing, and smishing. Key factors influencing vulnerability included age, education level, and security measures adopted. The findings underscore the need for targeted cybersecurity education, stricter regulatory frameworks, and improved security measures for mobile users. The study concludes with recommendations to enhance digital literacy, enforce stricter cybersecurity policies, and encourage the adoption of stronger security practices to mitigate social engineering risks.

Keywords: Social Engineering Attacks, Cybersecurity Awareness, Mobile Security, Phishing, Smishing.

1. INTRODUCTION

Social engineering attacks have emerged as one of the most prevalent and sophisticated cybersecurity threats in the digital age. Unlike conventional cyberattacks that exploit vulnerabilities in software or network systems, social engineering attacks target human psychology, manipulating individuals into revealing sensitive information or performing actions that compromise security. Attackers employ different enumeration techniques, such as sending phishing links and malicious payloads to collect victim's personal information (Al-Khateeb et al., 2023; Maraj & Butler, 2022; Rathod et al., 2025). As mobile devices become increasingly integrated into personal and professional activities, they have become a primary target for these attacks, exposing users to significant risks. Social engineering attacks have not been effectively addressed, in contrast to technological attacks that have been studied for decades (Patcha & Park, 2007; Lopes et al., 2024).

The rapid growth of mobile technology in Nigeria has brought immense benefits, enhancing communication, financial transactions, and access to information. However, this widespread adoption has also made mobile users highly susceptible to cyber threats. Social engineering attacks have been on the rise in Nigeria, with cybercriminals taking advantage of users' limited awareness and poor security practices to exploit vulnerabilities. Despite efforts by regulatory bodies such as the Nigerian Communications Commission (NCC) to promote cybersecurity awareness, many mobile users remain unaware of the various tactics employed by cybercriminals. As a result, financial fraud, identity theft, and emotional distress caused by social engineering attacks have continued to escalate.

The increasing reliance on mobile devices for financial transactions has made social engineering attacks particularly concerning. Mobile banking applications, digital wallets, and online payment platforms have simplified financial transactions, but they have also introduced new security risks. Cybercriminals exploit users' trust in these platforms by sending fraudulent messages, impersonating financial institutions, or creating fake login portals to steal credentials. Due to human interactions, social engineering attacks are the most powerful attacks because they threaten all systems and networks (Salahdine & Kaabouch, 2019). Phishing, smishing, and vishing are commonly used to trick unsuspecting users into disclosing sensitive information. The rise of digital fraud underscores the importance of strengthening security measures, educating users on cyber threats, and implementing policies that mitigate social engineering risks.

While many mobile users may recognize terms such as phishing or smishing, they often fail to take proactive steps to protect themselves from these threats. Research has shown that despite high awareness levels, a substantial proportion of users do not utilize security features such as two-factor authentication (2FA), strong passwords, or antivirus software. Additionally, many individuals underestimate their vulnerability, assuming that cybercriminals primarily target high-profile individuals or large corporations. This false sense of security increases susceptibility to attacks, making education and training essential components of cybersecurity strategies.

Existing literature on social engineering attacks highlights the psychological manipulation techniques used by cybercriminals to exploit human behavior. People are frequently the weakest link in an information system, and they can be persuaded or tricked into disclosing private information that gives unauthorized users access to systems that are protected (Mouton, 2017; Lopes et al., 2024). Attackers often use urgency, fear, curiosity, or authority to influence victims into acting impulsively. For instance, a smishing attack may involve a fraudulent SMS claiming that a bank account will be suspended unless the user verifies their details immediately. Similarly, vishing scams involve phone calls from fraudsters posing as customer service representatives to extract confidential information. These manipulative strategies emphasize the need for mobile users to exercise caution and verify the authenticity of messages or calls before responding.

Despite efforts by financial institutions and telecom providers to enhance security, the effectiveness of existing preventive measures remains uncertain. d by cyber attackers [5]. A cyber security attack was reported by Central Bank where an attacker stole over $80 million using a remote access trojans (RAT) installed on the bank's computers (Libicki, 2018; Salahdine & Kaabouch, 2019). This study seeks to assess the adequacy of current security practices adopted by mobile users in Edo State and determine whether they effectively mitigate social engineering risks. Understanding the effectiveness of security measures such as biometric authentication, encryption tools, and cybersecurity training programs will provide valuable understanding into how mobile security can be improved.

The consequences of social engineering attacks extend beyond individual victims to organizations and economies as a whole. To combat cyberattacks, the banking sector invests $274 billion globally (Acharya and Joshi, 2020; Orucho et al., 2023). Businesses that fall victim to these attacks may suffer financial losses, data breaches, and reputational harm, while governments must contend with the broader implications of cybercrime on national security and economic stability. Addressing the challenge of social engineering requires a multi-faceted approach that includes education, technological advancements, and regulatory measures. Raising public awareness about the tactics used by cybercriminals and encouraging the adoption of strong security practices can significantly reduce vulnerability to these attacks.

As cyber threats continue to evolve, ongoing research is essential to understanding emerging risks and developing effective countermeasures. By analyzing patterns of social engineering attacks and identifying the factors that contribute to user susceptibility, researchers and technology developers can work together to strengthen cybersecurity frameworks. The need for proactive measures has never been more critical, as the digital landscape continues to expand and cybercriminals refine their deceptive techniques to exploit human behavior. As cybercriminals develop more advanced techniques, mobile users must be equipped with adaptive security measures that evolve alongside emerging threats. The results of this study will provide a foundation for future research, guiding efforts to strengthen mobile security and mitigate the impact of social engineering attacks in Nigeria and beyond.

2. RESEARCH METHODOLOGY

2.1 Study Area

The study was conducted in Edo State, Nigeria, a region known for its economic activities, educational institutions, and diverse population. Edo State comprises urban, semi-urban, and rural areas, making it an ideal location to assess the vulnerability and impact of social engineering attacks on mobile users across different demographic groups. The research focused on three key locations: Benin City, Uromi, and Ewohimi. Benin City, the state capital, represents an urban setting with a high concentration of mobile users engaged in various digital transactions. Uromi, a semi-urban town, provided perception into social engineering vulnerabilities in a developing commercial hub. Ewohimi, a rural area, allowed for an understanding of security awareness levels in less technologically advanced communities. These locations were strategically selected to ensure a comprehensive analysis of how social engineering attacks affected mobile users with varying access to digital literacy, financial resources, and cybersecurity awareness.

2.2 Method of Data Collection

The study employed a structured questionnaire as the primary data collection instrument to assess the vulnerability and impact of social engineering attacks on mobile users in Edo State. A stratified random sampling technique was utilized to ensure adequate representation across different demographic segments. The study targeted mobile users in three key locations—Benin City, Uromi, and Ewohimi—representing urban, semi-urban, and rural settings, respectively. The questionnaire comprised both closed-ended and open-ended questions designed to capture respondents' awareness levels, experiences with social engineering attacks, security practices, and the financial and personal impacts of such attacks. Data collection was conducted through multiple channels, including face-to-face interviews, online surveys, and printed questionnaire distribution at strategic locations such as universities, markets, and business centers.

2.3 Sample Size and Sampling Technique

The study employed a stratified random sampling technique to ensure adequate representation of mobile users across different demographic groups in Edo State. Stratification was based on geographic location, covering urban (Benin City), semi-urban (Uromi), and rural (Ewohimi) areas to capture diverse experiences with social engineering attacks. This approach allowed for a balanced analysis of awareness levels, attack exposure, and security practices among different population segments. A total of 280 structured questionnaires were distributed across the three selected locations, targeting individuals who actively use mobile devices for communication, banking, and other digital transactions. Out of these, 267 completed questionnaires were successfully retrieved, resulting in a high response rate of 95.36%. This ensured a robust dataset for analysis.

2.4 Data Analysis

The collected data were analyzed using descriptive statistics and multiple regression analysis to assess the vulnerability and impact of social engineering attacks on mobile users in Edo State. Descriptive statistics, including frequencies, percentages and means, were used to summarize respondents' awareness levels, experiences with social engineering attacks, and security practices. These statistical measures provided awareness into the distribution of responses and helped identify key patterns and trends among mobile users in different demographic segments.

For inferential analysis, multiple regression analysis was employed to examine the relationship between users' demographic characteristics, awareness levels, security practices, and their susceptibility to social engineering attacks. The regression model used in the study was specified as follows:

$Y = \beta_0 + \beta_1X_1 + \beta_2X_2 + \beta_3X_3 + \beta_4X_4 + \beta_5X_5 + \epsilon$

Where:

- Y = Susceptibility to social engineering attacks (dependent variable)
- X_1 = Awareness level of social engineering threats
- X_2 = Security measures adopted (e.g., use of antivirus, two-factor authentication)
- X_3 = Frequency of exposure to suspicious messages/calls
- X_4 = Educational level of the respondent
- X_5 = Age of the respondent
- β_0 = Intercept
- $\beta_1 - \beta_5$ = Regression coefficients
- ϵ = Error term

The regression analysis tested the significance of these independent variables in predicting mobile users' vulnerability to social engineering attacks. The coefficient of determination (R2R^2R2) was used to measure the proportion of variance in susceptibility explained by the predictor variables. A p-value < 0.05 was considered statistically significant, indicating strong associations between specific factors and vulnerability to attacks.

3. RESULTS AND DISCUSSION

3.1 Results

The study analyzed responses from 267 mobile users in Edo State to assess their vulnerability and experiences with social engineering attacks. The findings are summarized in tables, highlighting demographic distribution, awareness levels, security practices, and recommendations for improving mobile security.

Table 1 indicates that the majority of respondents (30.3%) were aged 26–35 years, followed by 18–25 years (27.3%). Table 2 shows that 63% of respondents were male, while 37% were female. Table 3 reveals that 47% of respondents resided in Benin City, 37% in Uromi, and 16% in Ewohimi. Table 4 highlights that most respondents (67%) had tertiary education, while 33% had secondary or primary education. Table 5 shows that 39% of respondents were students, followed by unemployed individuals (22.8%) and business owners (13.9%).

Table 1: Age group of Respondents

Years	Frequency	Percentage	Cumulative Percentage
18 – 25	73	27.3	27.3
26 – 35	81	30.3	57.6
36 – 45	59	22.1	79.7
46 – 55	44	16.5	96.2
Above 55	10	3.7	100
Total	267	100	

Source: Field Data, 2025

Table 2: Gender of Respondents

Gender	Frequency	Percentage	Cumulative Percentage
Male	168	63.0	63.0
Female	99	37.0	100
Total	267	100	

Source: Field Data, 2025

Table 3: Location of Respondents

Location	Frequency	Percentage	Cumulative Percentage
Benin City	125	47.0	47.0
Uromi	98	37.0	84.0
Ewohimi	44	16.0	100
Total	267	100	

Source: Field Data, 2025

Table 4: Education Qualification of Respondents

Education Qualification	Frequency	Percentage	Cumulative Percentage
Primary Education	32	12.0	12.0
Secondary Education	56	21.0	33.0
Tertiary Education (Undergraduate)	89	33.3	66.3
Tertiary Education (postgraduate)	90	33.7	100
Total	267	100	

Source: Field Data, 2025

Table 5: Occupation of Respondents

Occupation	Frequency	Percentage	Cumulative Percentage
Student	104	39.0	39.0
Professional	30	11.2	50.2
Business Owner	37	13.9	64.1
Employee	35	13.1	77.2
Unemployed	61	22.8	100
Total	267	100	

Source: Field Data, 2025

Table 6 indicates that 88.4% of respondents were aware of social engineering attacks, with the majority learning about them from the internet (44.5%). The most recognized tactics included smishing (31.4%), vishing (25.4%), and phishing (19%). Despite this, 34.5% of respondents believed they were vulnerable, while 44.9% were uncertain.

Table 6: Awareness of Social Engineering Attacks

Are you aware of social engineering attacks?	Frequency	Percentage	Cumulative Percentage
Yes	236	88.4	88.4
No	31	11.6	100
Total	267	100	

How did you first learn about social engineering attacks	**Frequency**	**Percentage**	**Cumulative Percentage**
Media (TV, Radio, etc)	69	29.2	29.2
Internet (websites, social media, etc)	105	44.5	73.7
Friends or family	35	14.8	88.5
Educational Institutions	27	11.4	100
Total	236	100	
Which of the following social engineering tactics are you familiar with?	**Frequency**	**Percentage**	**Cumulative Percentage**
Phishing (fraudulent emails)	66	19.0	19.0
Vishing (fraudulent phone calls)	88	25.4	44.4
Smishing (fraudulent sms)	109	31.4	75.8
Baiting (fraudulent offers)	44	12.7	88.5
Pretexting (impersonation)	40	11.5	100
Total	347	100	
Do you think you are vulnerable to social engineering attacks?	**Frequency**	**Percentage**	**Cumulative Percentage**
Yes	92	34.5	34.5
No	55	20.6	55.1
Not Sure	120	44.9	100
Total	267	100	

Source: Field Data, 2025

Table 7 reveals that 51.3% of respondents had experienced social engineering attacks, with smishing (27.9%) and vishing (23.8%) being the most common. The impact included financial loss (38.9%), emotional distress (26.4%), and identity theft (20.1%). Additionally, 28.8% of respondents reported frequent exposure to suspicious messages or calls.

Table 7: Experience with Social Engineering Attacks

Have you ever experienced any social engineering attack?	**Frequency**	**Percentage**	**Cumulative Percentage**
Yes	121	51.3	51.3
No	115	48.7	100
Total	236	100	
If yes, which type of attack did you experience?	**Frequency**	**Percentage**	**Cumulative Percentage**
Phishing	32	18.6	18.6
Vishing	41	23.8	42.4
Smishing	48	27.9	70.3
Baiting	28	16.3	86.6
Pretexting	23	13.4	100
Total	172	100	
What was the outcome of the attack?	**Frequency**	**Percentage**	**Cumulative Percentage**

Financial loss	56	38.9	38.9
Identity theft	29	20.1	59.0
Emotional distress	38	26.4	85.4
No impact	21	14.6	100
Total	144	100	
How frequently do you receive suspicious messages or calls (e.g., unsolicited requests for personal information, money)?	**Frequency**	**Percentage**	**Cumulative Percentage**
Never	115	48.7	48.7
Occasionally	29	12.3	61
Frequently	68	28.8	89.8
Always	24	10.2	100
Total	236	100	

Source: Field Data, 2025

Table 8 shows that 40.5% of respondents did not use any security measures, while only 26.1% used secure passwords and 19.6% adopted two-factor authentication (2FA). Despite this, 52.8% considered these measures effective. However, only 11.6% had received training on mobile security, with 83.9% of training programs provided by employers.

Table 8: Security Measures and Practices

Do you currently use any security measures on your mobile device?	**Frequency**	**Percentage**	**Cumulative Percentage**
Antivirus software	21	6.2	6.2
Two-Factor Authentication (2FA)	67	19.6	25.8
Secure passwords	89	26.1	51.9
Encryption tools	26	7.6	59.5
None	138	40.5	100
Total	341		
How effective do you think these security measures are in preventing social engineering attacks?	**Frequency**	**Percentage**	**Cumulative Percentage**
Very effective	102	52.8	52.8
Somewhat effective	56	29.0	81.8
Not effective	8	4.1	85.9
Don’t know	27	14.0	100
Total	193	100	
Have you ever received any training or awareness programs regarding mobile security?	**Frequency**	**Percentage**	**Cumulative Percentage**
Yes	31	11.6	11.6
No	236	88.4	100
Total	267	100	

If yes, who conducted the training or awareness program?	Frequency	Percentage	Cumulative Percentage
Employer/Organization	26	83.9	83.9
School/University	3	9.7	93.6
Government/NGO	2	6.5	100
Total	31	100	

Source: Field Data, 2025

Table 9 indicates that 51.3% of respondents advocated for more training and awareness campaigns, while 22.5% supported stricter regulations. Notably, all respondents expressed willingness to participate in future training programs.

Table 9: Recommendations for Improved Mobile Security

What steps do you think can be taken to improve mobile security awareness among users in Edo State?	Frequency	Percentage	Cumulative Percentage
More training and awareness campaign	137	51.3	51.3
Stricter regulations and enforcement	60	22.5	73.8
Enhanced mobile security features from service providers	42	15.7	89.5
Community-based security programs	28	10.5	100
Total	267	100	
Would you be willing to participate in future training or awareness campaigns on mobile security?	**Frequency**	**Percentage**	**Cumulative Percentage**
Yes	267	100	100
No	0	0.0	100
Total	267	100	

Source: Field Data, 2025

The multiple regression analysis examined the relationship between mobile users' susceptibility to social engineering attacks and key predictor variables, including awareness level, security measures adopted, exposure frequency, education level, and age.

Table 10: Multiple regression analysis

Predictor variable	Coefficient (β)	Std. Error	p-Value
Intercept ($\beta_{0)}$	2.551	0.251	0.001
Awareness Level (X_1)	-0.0278	0.117	0.812
Security Measures (X_2)	-1.2977	0.171	0.002
Exposure Frequency (X_3)	0.0502	0.103	0.625
Education Level (X_4)	-0.4492	0.061	0.003
Age (X_5)	0.2650	0.068	0.002

Regression Equation:

$$Y = 2.551 - 0.0278X_1 - 1.2977X_2 + 0.0502X_3 - 0.4492X_4 + 0.2650X_5 + \epsilon$$

3.2 Discussion

The findings of this study underscore the complex interplay between demographic factors, awareness levels, security practices, and susceptibility to social engineering attacks among mobile users in Edo State. The demographic distribution revealed that a significant proportion of respondents were within the age range of 26–35 years (30.3%), followed closely by the 18–25 age group (27.3%). This suggests that younger and middle-aged individuals, who are more likely to engage in digital transactions and online communication, constitute a large share of mobile users. Additionally, the higher proportion of male respondents (63%) compared to females (37%) may reflect the general trend in mobile technology adoption and engagement in cybersecurity-related discussions. The regional distribution of respondents, with 47% from Benin City, 37% from Uromi, and 16% from Ewohimi, ensured a balanced representation of urban, semi-urban, and rural experiences.

The awareness of social engineering attacks was found to be relatively high, with 88.4% of respondents indicating that they were familiar with the concept. However, despite this level of awareness, a substantial proportion of respondents (44.9%) remained unsure of their vulnerability, while 34.5% admitted to feeling susceptible to such attacks. This highlights the disconnect between theoretical awareness and practical security preparedness. The primary source of awareness was the internet (44.5%), followed by media sources such as television and radio (29.2%), while formal education contributed the least (11.4%). This indicates that cybersecurity education within formal institutions remains limited and suggests that awareness campaigns should leverage digital platforms for maximum reach. The study also identified smishing (31.4%) as the most commonly recognized form of social engineering, followed by vishing (25.4%) and phishing (19%). The relatively high recognition of smishing aligns with the increasing reliance on mobile communication and SMS-based fraud tactics.

The prevalence of social engineering attacks was evident, as 51.3% of respondents had experienced such incidents. Among these, smishing (27.9%) and vishing (23.8%) were the most frequently reported attack types. The impact of these attacks was significant, with 38.9% of affected respondents suffering financial losses, 26.4% experiencing emotional distress, and 20.1% falling victim to identity theft. The financial implications of these attacks suggest that cybercriminals primarily exploit mobile users for economic gain. Additionally, the high incidence of emotional distress highlights the psychological toll of cybersecurity breaches, which can erode users' trust in digital platforms and hinder broader technological adoption. The frequency of suspicious messages or calls was another critical finding, with 28.8% of respondents receiving fraudulent communications frequently, and 10.2% reporting that they always encountered such threats. These results emphasize the persistent nature of social engineering threats and the need for proactive measures to mitigate them.

Security practices among respondents were found to be inadequate, with 40.5% admitting to not using any form of security measure. Among those who implemented protective measures, secure passwords (26.1%) and two-factor authentication (19.6%) were the most common. Despite the limited adoption of security measures, 52.8% of respondents believed that these tools were very effective in preventing social engineering attacks. However, the study also revealed a significant gap in formal cybersecurity training, as only 11.6% of respondents had received any form of security awareness education. The majority of training programs were provided by employers (83.9%), while government and educational institutions contributed minimally. This suggests that public and institutional cybersecurity initiatives need to be expanded to enhance digital literacy and threat mitigation strategies.

The regression analysis provided further awareness into the factors influencing susceptibility to social engineering attacks. Security measures had the most significant negative impact on vulnerability ($\beta = -1.2977$, $p < 0.002$), indicating that individuals who actively adopted protective measures were less likely to fall victim to such attacks. This reinforces the importance of encouraging stronger security practices among mobile users. Education level also played a critical role ($\beta = -0.4492$, $p < 0.003$), with higher educational attainment being associated with reduced susceptibility. This finding aligns with existing literature suggesting that individuals with greater digital literacy and cybersecurity awareness are better equipped to recognize and avoid fraudulent schemes. Conversely, age had a positive coefficient ($\beta = 0.2650$, $p < 0.002$), suggesting that older individuals were more vulnerable to social engineering attacks. This may be attributed to lower familiarity with emerging digital threats and reduced adaptability to evolving security practices.

Interestingly, awareness level ($\beta = -0.0278$, $p = 0.812$) was not found to be a significant predictor of vulnerability. This suggests that merely being aware of social engineering threats does not necessarily translate into effective risk mitigation. Instead, practical knowledge and proactive security behaviors are more critical in preventing attacks. Similarly, the frequency of exposure to suspicious messages or calls ($\beta = 0.0502$, $p = 0.625$) did not significantly influence susceptibility, indicating that repeated exposure alone does not directly correlate with falling victim to an attack. These findings suggest that user behaviour and engagement with security measures are more influential factors in cybersecurity resilience than passive awareness or exposure levels.

4. CONCLUSION

The study has provided valuable knowledge into the vulnerability and impact of social engineering attacks on mobile users in Edo State. It has highlighted the critical role of security practices, education, and demographic factors in determining susceptibility to such attacks. While awareness of social engineering threats was relatively high among respondents, the findings indicated that awareness alone does not necessarily translate into effective prevention. Instead, practical security measures such as strong passwords, two-factor authentication, and cybersecurity training played a more significant role in reducing vulnerability. The study also revealed that older individuals were more susceptible to social engineering attacks, emphasizing the need for targeted educational interventions for this demographic group. Moreover, the prevalence of financial loss and emotional distress as consequences of these attacks underscores the urgency of implementing stronger cybersecurity policies and awareness campaigns. Given the increasing sophistication of cybercriminal tactics, there is a pressing need for continuous cybersecurity education and policy enforcement to safeguard mobile users in Edo State.

5. RECOMMENDATIONS

The study proposed the following recommendations based on the findings:

1. **Strengthening Cybersecurity Awareness Programs:** Government agencies, educational institutions, and mobile service providers should collaborate to develop comprehensive awareness campaigns tailored to different user demographics, ensuring practical knowledge of cybersecurity threats and prevention strategies.
2. **Encouraging the Adoption of Security Measures:** Mobile users should be encouraged to implement strong security practices such as secure passwords, two-factor authentication, and encryption tools to mitigate their risk of falling victim to social engineering attacks.
3. **Integrating Cybersecurity Education into Formal Curriculum:** Schools and universities should incorporate cybersecurity awareness training into their curricula to equip students with essential skills for identifying and mitigating cyber threats.
4. **Expanding Training Initiatives for Older Users:** Given the increased vulnerability of older individuals, targeted training programs should be designed to improve their digital literacy and equip them with practical skills for recognizing and avoiding social engineering scams.
5. **Encouraging Community-Based Cybersecurity Support Groups:** Local cybersecurity initiatives, such as community forums and digital literacy workshops, should be promoted to create an interactive platform where users can share experiences, report cyber threats, and receive expert guidance on best security practices.

ACKNOWLEDGEMENT

The authors sincerely appreciate the leadership of the National Institute of Construction Technology and Management (NICTM), Uromi, and the Tertiary Education Trust Fund (TETFund) for their generous financial support, which played a crucial role in the successful completion of this research project.

REFERENCE

1. Acharya, S., & Joshi, S. (2020). Impact of cyber-attacks on banking institutions in India: A study of safety mechanisms and prevention measures. *Palarch's Journal of Archeology of Egypt, 17*(6), 4656-4670.
2. Al-Khateeb, M., Al-Mousa, M., Al-Sherideh, A., Almajali, D., Asassfeha, M., & Khafajeh, H. (2023). Awareness model for minimizing the effects of social engineering attacks in web applications. *International Journal of Data and Network Science, 7*(2), 791–800.
3. Libicki, M. (2018). Could the issue of DPRK hacking benefit from benign neglect? *Georgia Journal of International Affairs, 19*, 83–89.
4. Lopes, A., Mamede, H. S., Reis, L., & Santos, A. (2024). Common techniques, success attack factors, and obstacles to social engineering: A systematic literature review. *Emerging Science Journal, 8*(2), 761-778.
5. Maraj, A., & Butler, W. (2022). Taxonomy of social engineering attacks: A survey of trends and future directions. *International Conference on Cyber Warfare and Security, 17*, 185–193.
6. Mouton, F., Nottingham, A., Leenen, L., & Venter, H. S. (2017). Underlying finite state machine for the social engineering attack detection model. *Information Security for South Africa (ISSA), Johannesburg, South Africa*.
7. Orucho, D. O., Awuor, F. M., Ratemo, C., & Oduor, C. (2023). Security threats affecting user-data on transit in mobile banking applications: A review. *International Journal of Computer Engineering Research, 9*(1), 1-11.
8. Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks, 51*(12), 3448-3470.
9. Rathod, T., Jadav, N. K., Tanwar, S., Alabdulatif, A., Garg, D., & Singh, A. (2025). A comprehensive survey on social engineering attacks, countermeasures, case study, and research challenges. *Information Processing and Management, 62*, 103928.
10. Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet, 11*(4), 89.