Quantitative Evaluation of Social Engineering Attacks and their Impact on the Financial Services Sector

Abstract

This study evaluates the impact of social engineering (SE) attack techniques on the financial sector, focusing on financial losses, reputational harm, regulatory consequences, operational disruptions, and privacy violations. Using a mixed-methods approach that combines literature review, survey questionnaires, and interviews with financial institutions and customers, the research introduces a Social Engineering Impact Index (SEII) for quantifying vulnerabilities. Findings reveal that financial institutions face high to extremely high levels of SE attack impact, with personal financial information (PFI) theft and direct monetary loss being the most significant contributors. The study emphasizes the need for enhanced employee training, customer awareness, advanced fraud detection, and strong incident response strategies. The proposed SEII framework provides a practical tool for measuring SE attack risks and guiding policy interventions.

Keywords: *social engineering, impact, financial services, social engineering impact index,social engineering impact measure*

Introduction

Social engineering (SE) attacks have emerged as one of the most pervasive and damaging forms of cyber threats facing financial institutions. Unlike traditional cyberattacks that exploit technical flaws, SE attacks exploit human psychology, trust, and behavioral vulnerabilities [1].Attackers rely on manipulation techniques—such as phishing, vishing, smishing, and pretexting—to deceive employees or customers into disclosing sensitive information or performing harmful actions [2].The financial sector is particularly vulnerable due to its dependence on customer trust and its custody of sensitive personal and financial data. Attacks such as the Carbanak gang's global campaign, which resulted in losses exceeding $1 billion [3], highlight the scale of financial damage possible. Similarly, the 2017 Equifax breach demonstrated how SE-related techniques can compromise millions of individuals' personal data, with long-term reputational and regulatory consequences [4].

These incidents underscore the multidimensional impacts of SE attacks: direct financial loss, erosion of trust, privacy violations, and operational disruptions. Moreover, regulatory pressures compel financial institutions to comply with stringent cybersecurity standards, and failure often results in fines and legal actions [5]. Thus, SE attacks not only threaten organizational viability but also destabilize public confidence in financial markets.Despite these challenges, literature suggests that SE attacks are often underestimated due to the intangible nature of psychological exploitation [6]. While technical defenses against cyberattacks are well established, the human factor remains the weakest link in cybersecurity. Consequently, assessing and quantifying the impact of SE attacks is vital for developing robust countermeasures.

This study addresses this gap by developing a Social Engineering Impact Index (SEII) that categorizes vulnerabilities and measures impacts across privacy, economic, and trust dimensions. The research aims to provide empirical evidence from Nigerian financial institutions, enabling stakeholders to make informed security and policy decisions.

Scholars have consistently identified SE as a leading cybersecurity challenge. [7highlighted why phishing succeeds by exploiting cognitive biases, while [8explained how pretexting manipulates trust relationships. More recent studies emphasize the growing sophistication of SE techniques in financial services, with tailored attacks such as spear-phishing and business email compromise (BEC) causing billions in annual losses [9] and [10]Research on the impacts of SE has categorized consequences into three broad areas: (1) economic and financial losses, (2) erosion of customer trust, and (3) privacy violations [11] and [12]. Economic impacts include stolen funds, litigation costs, and compliance penalties [13]. Trust erosion leads to customer abandonment and damaged institutional reputation [14].Privacy violations, often linked to personal identifiable information (PII) and PFI theft, amplify both economic and reputational harm [12].

Theoretical perspectives also explain SE dynamics. Cognitive dissonance theory describes how attackers induce psychological discomfort to manipulate decisions [15]Information processing theory shows how biases influence victim susceptibility [16]. Behavioral economics links attacker strategies to irrational decision-making under fear or urgency [17].Despite these insights, literature gaps remain. First, limited quantitative frameworks exist for measuring SE impacts. Second, financial sector-specific analyses are scarce, even though banks and insurance firms are prime targets [18]. Third, few studies explore long-term consequences, such as brand damage and customer trust erosion. This study addresses these gaps by providing a quantitative model for SE impact measurement using data from Nigerian banks.

Several empirical studies confirm the severity of SE in financial systems. [13] reported that Nigerian banks face continuous SE-related losses, with phishing and fraudulent mobile transactions being the most prevalent. [19] highlighted that social networks amplify SE risks, providing attackers with fertile ground for phishing and impersonation. Similarly, [14]proposed a user-reflective model for mitigating SE attacks in the New Zealand banking system, emphasizing customer awareness as a key defense.

Other studies have focused on detection and prediction. [20]demonstrated that machine learning can predict individuals' susceptibility to SE, offering proactive prevention mechanisms. [1], however, observed that even highly trained staff remain vulnerable due to cognitive and organizational factors, suggesting that training alone is insufficient without cultural change. [6] proposed an extended SE attack framework that models each stage of manipulation, from information gathering to execution, showing how attackers exploit both technology and psychology.Collectively, these studies establish that while the methods of SE are well understood, few works provide a quantitative measure of impact. This dissertation addresses that gap by introducing metrics and computational models tailored to the financial sector.

To address the gaps identified, the following research questions guided the authors: What are the factors responsible for social engineering attacks on the financial services sector? How can these factors be measured for the purpose of the evaluation of the impact of social engineering attacks on the financial services sector? What are the metrics for quantifying the impact of social engineering attacks on the financial services sector?The rest of the article is organised into: section 2, presenting the background and related works, section 3, materials and methods, section 4, presents the social engineering impact index (SEII) framework,and model, section 5 is the data presentation while section concludes the paper with discussions and findings.

Methodology

The research adopted the pragmatic philosophical paradigm, enabling the integration of both qualitative and quantitative approaches [21]. A mixed-methods strategy was used thus: Qualitative**:** Literature was reviewed to identify metrics for SE impacts, including financial loss, PII/PFI theft, and trust erosion.Quantitative**:** A structured survey instrument, the Social Engineering Attacks Impact Questionnaire (SEAIQ), was distributed to employees of 20 banks in Abuja. Complementary interviews were conducted with cybersecurity officers.Sampling**:** Purposive sampling was applied to select banks and employees due to time and cost constraints.Analysis**:** Data was processed using exploratory data analysis (EDA) techniques, leading to the development of the Social Engineering Impact Index (SEII), which aggregates Privacy Impact (PI), Economic and Financial Impact (EFI), and Erosion of Trust Impact (ETI).

Results

Design of Social Engineering Impact Framework

Figure 1 presents a framework depicting the layers of the various metrics that supported the quantification of the impact of social engineering attacks on the financial services sector.

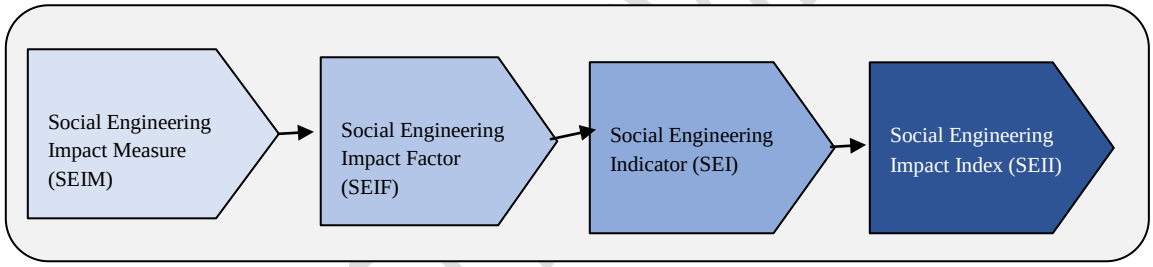


Figure 1: Social Engineering Attacks Impact Assessment Framework

The social engineering impact index (SEII) is the overall measurement that this work intends to achieve, it communicates the overarching impact of social engineering attacks on the financial sector. However, it requires values from a lower metric, namely; social engineering indicator, the SEI obtains it value from the aggregate values of the social engineering impact factor (SEIF). The SEIF on the other hand obtains its quantitative values from the actual impact measured with. Figure 2 further extend the framework in Figure 1 to show the sub-metrics under each of the layers. Tables 1-3 on the other hand present the granular scales for quantitative assessment of the metrics in the various SEIs.

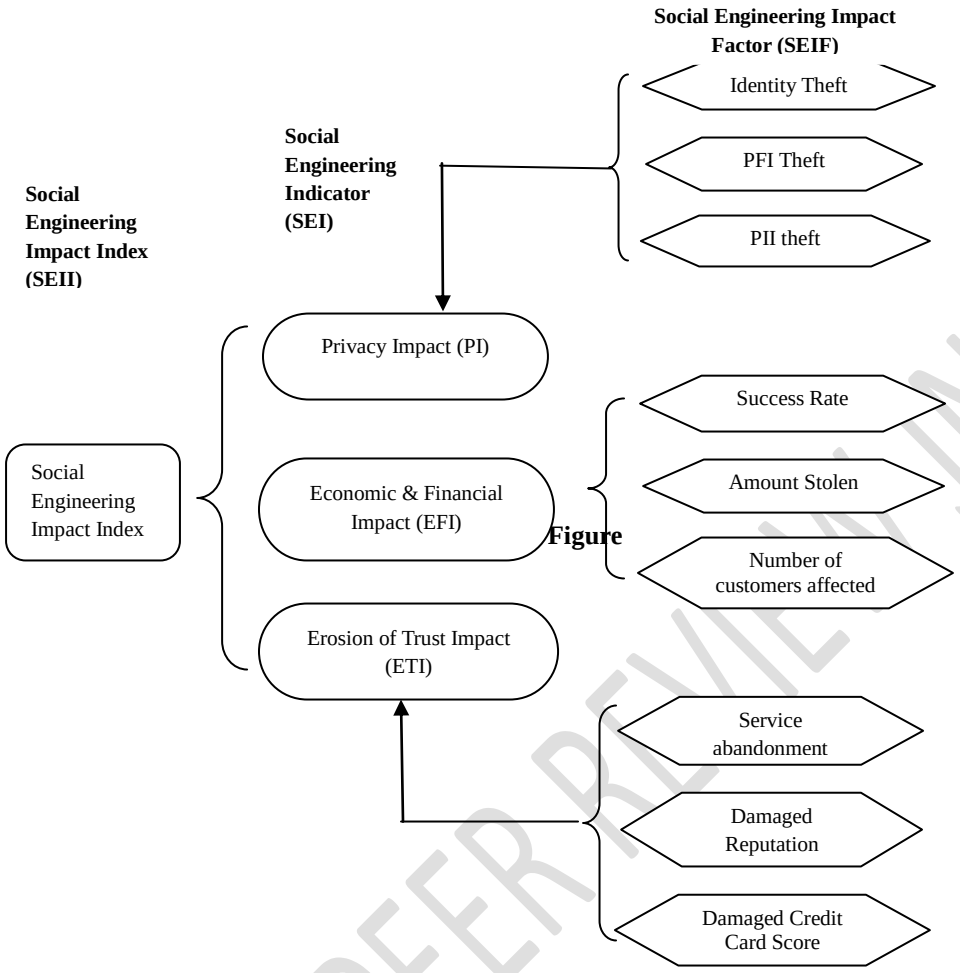


Figure 2: Expansion of Social Engineering Attacks Impact Assessment Framework

In Figure 2, three SEI are derived from the SEII, namely; privacy impact (PI), economic and financial impact (EFI) and erosion of trust impact (ETI). The PI measures the impact of social engineering attacks on privacy of individuals especially as it is associated with the personal financial information (PFI). The EFI measures the economic and financial impacts on the financial institutions and customers with respect to the value of monies lost as a result of social engineering attacks. The third sub-metric, which is the ETI measures the extent to which trust is eroded in the digital financial systems as a result of social engineering attacks. Three SEIF are derived from each of the SEI as illustrated in Figure 2. The idea is to deepen the measurements and arrive at a granular level of measurement. Under PI, the sub-metrics considered are; identity theft, personal financial information (PFI) theft, personal identifiable information (PII) theft. In EFI, success rate, i.e, the rate at which social engineering attacks succeed, the amount stolen (value) during successful attacks, and number customers successfully attacked using SE form the basis for the measurement. From the ETI, the impact on the financial instructions such as distrust, leading to service abandonments and damaged reputation are measured; similar, the impact on the customer measured in terms of damaged credit card history as a result of the attackers using their credit card to borrow money beyond the capacity of the victim to pay within reasonable time forms part of the measurement.

Social Engineering Impact Measure (SEIM) Scale

The SEIM scale provides the granular measure of the impact of social engineering attacks on financial institutions. It is presented in Table 1 on a five-point scale of 1-5 where 1 is the least (minimal) impact experienced and 5 is the most severe impact experienced. As a result of the different variables of measuring the impact if SE attacks on the financial services sector, Table 1 is extended as presented in Table 2-4

Table 1: Social Engineering Impact Quantification Scale

#	Qualitative	Description	Weight
1	Minimal	Negligible impact, unlikely to cause disruption; requires little to no intervention. Risk is virtually inconsequential, with only routine monitoring needed.	1
2	Low	Minor impact, manageable with minimal disruption. Some attention may be warranted, but issues are easily recoverable and pose minimal risk to operations.	2
3	Moderate	Noticeable impact, potentially affecting operations. Attention is necessary to prevent escalation; requires reasonable resources to mitigate, though still manageable with standard intervention.	3
4	High	Significant impact with likely operational, financial, or security consequences. Requires prompt attention and substantial resources, as potential for harm or disruption is high.	4
5	Extremely High	Critical impact, potentially catastrophic. Immediate, intensive action is essential to prevent extensive damage, disruption, or harm, often necessitating an all-encompassing response.	5

Source: [22], [23]

Table 2: Privacy Impact

Variable	Range (₦)	Qualitative	Weight
Identity theft	1-20	Minimal	1
	21-40	Low	2
	41-60	Moderate	3
	61-80	High	4
	81^{+}	Extremely High	5
	Range (₦)	**Qualitative**	
Personal Financial Information (PFI) theft	1-20	Minimal	1
	21-40	Low	2
	41-60	Moderate	3
	61-80	High	4
	81^{+}	Extremely High	5
	Range (₦)	**Quantitative**	**Weight**
Personal Identifiable Information (PII) theft	1-20	Minimal	1
	21-40	Low	2
	41-60	Moderate	3
	61-80	High	4
	81^{+}	Extremely High	5

Source [24], [25]

Table 3: Economic and Financial Impact

Variable	Range (₦)	Qualitative	Weight
Amount Lost	1-199,000	Minimal	1
	200,000-499,000	Low	2
	500,000 – 1,500,000	Moderate	3
	1,501,000 – 2,000,000	High	4
	2,000,0000+	Extremely High	5
	Range	**Qualitative**	
Number of Customers Affected	1-20	Minimal	1
	21-40	Low	2
	41-60	Moderate	3
	61-80	High	4
	81^{+}	Extremely High	5
	Rate (%)	**Qualitative**	
Succes Rate	1-20	Minimal	1
	21-40	Low	2
	41-60	Moderate	3
	61-80	High	4
	81^{+}	Extremely High	5

Source [26]

Table 4: Erosion of Trust Impact

Variable	Rate (%)	Qualitative	Scale
Service Abandonment	1-20	Minimal	1
	21-40	Low	2
	41-60	Moderate	3
	61-80	High	4
	81^{+}	Extremely High	5
	Monetary value of damaged reputation	**Qualitative value**	**Weight**
Damaged Reputation	1-199,000	Minimal	1
	200,000-499,000	Low	2
	500,000 – 1,500,000	Moderate	3
	1,501,000 – 2,000,000	High	4
	2,000,0000+	Extremely High	5
	Credit points		**Weight**
Damaged credit card Score	800^{+}	Exception	1
	799-740	Very Good	2
	739-670	Good	3
	669-580	Fair	4
	579^{-}	Poor	5

Source: [27], [28], [29]

Although reputation itself is considered an intangible asset, it damaged can be quantitatively managed in terms of the monetary values associated with its effects, namely; lost revenue; changes or increases in capital; operating; or regulatory costs; or significant decreases in shareholder value. Thus, it is measured in Table 4 with respect to the cost in quantitative ranges.

Impact of Social Engineering Attacks Computation

To compute the quantitative value of the impact of social engineering attacks on the financial services sector, the following variables are defined as derived from Figure 2.

i. Social Engineering Impact Measure (SEIM) under each SEIF the granular measure of the impact of the impact of social engineering defined in Table 1 on a scale of 1-5.
ii. Social Engineering Impact Factor (SEIF) is the summation of the granular values of Social Engineering Impact Measure (SEIM) under each SEIF.
iii. social engineering indicators (SEI) is the summation of the Social Engineering Impact Factor (SEIF) under each SEI.
iv. Social Engineering Impact Index (SEII) is the summation of the social engineering indicators (SEI)

Derivation of equation

$$SEIF = \sum SEIM \quad \text{Equation (1)}$$

$$SEI = \sum SEIF \quad \text{Equation (2)}$$

$$SEII = \sum SEI \quad \text{Equation (3)}$$

Since the value of each computation is to be kept between 00.00 – 1.00 as described in Table 5, the sigmoid function is applied to normalise the values between 00.00 – 1.00. The sigmoid function is reproduced below:

$$\sigma(x) = 1/1+e^{-x}$$

x is the input variable (a real number), in this case the unnormalized values of SEIF, SEI and SEII
e is Euler's number (approximately **2.71828**), the base of natural logarithms
$\sigma(x)$ is the normalised value of SEIF, SEI or SEII

The formula computes the sigmoid or logistic function, commonly used in machine learning and neural networks

Impact Categorisation (levels)

To comparative understand the effect of the computed impacts, they will be categorised to enable a clear view and understanding. Thus, the computed impact at various levels, namely SEII, SEI and SEIF will be categorised on a 5-band scale as shown in Table 5 referred to as impact category. This conforms to the impact measure scale presented in Table 1. Based on this, five impact categories are defined as IC_1 (0.00 – 0.20), IC_2 (0.21 -0.40), IC_3 (0.41-0.60), IC_4 (0.61-0.80) and IC_5 (0.81-1.00) the description and explanations are elaborated in Table 3.

Table 5: Impact Categorisation (Levels)

#	Impact Category (IC)	Description	Explanation
1	0.00 – 0.20	Minimal	Negligible change, insignificant influence or effects
2	0.21 – 0.40	Low	Inadequate enforcement, insufficient penalties, ineffective deterrence and limited compliance.
3	0.41 – 0.60	Moderate	Partial compliance, moderate enforcement, mixed outcomes and limited efficacy.
4	0.61 – 0.80	High	Comprehensive compliance, strong enforcement, clear regulations, significant penalties and effective deterrence.
5	0.81 – 1.00	Extremely High	Unwavering compliance, rigorous enforcement, explicit regulations, severe penalties and transformative deterrence.

Source: modified from [30], [31]

Data Presentation

Table 6 presents data on bank employees' awareness, vulnerability and organisational culture (AVOC). This is broken down to 3 items, namely; Awareness of Social Engineering Techniques (ASET), their vulnerability to social engineering technique (VSET) and employee behaviour and organisational culture (EBOC) as presented in Table 6.

Table 6: Awareness, Vulnerability and Organisational Culture

BankCode	ASET	VSEA	EBOC	AVOC
BANK 001	0.73	0.80	0.87	0.80
BANK 002	0.67	0.73	0.93	0.78
BANK 003	0.73	0.87	0.53	0.71
BANK 004	1.00	0.67	0.73	0.80
BANK 005	0.60	0.73	0.93	0.76
BANK 006	0.67	0.73	0.93	0.78
BANK 007	0.80	0.93	0.80	0.84
BANK 008	0.87	0.67	0.67	0.73
BANK 009	0.80	0.73	0.73	0.76
BANK 010	0.67	0.80	1.00	0.82
BANK 011	0.73	0.80	0.73	0.76
BANK 012	0.73	0.73	0.67	0.71
BANK 013	0.87	0.93	0.87	0.89
BANK 014	0.93	0.73	0.93	0.87
BANK 015	0.67	0.73	0.80	0.73
BANK 016	0.67	0.67	0.67	0.67
BANK 017	0.73	0.80	0.87	0.80
BANK 018	0.93	0.73	0.93	0.87
BANK 019	0.67	0.73	0.87	0.76
BANK 020	0.73	0.87	0.87	0.82

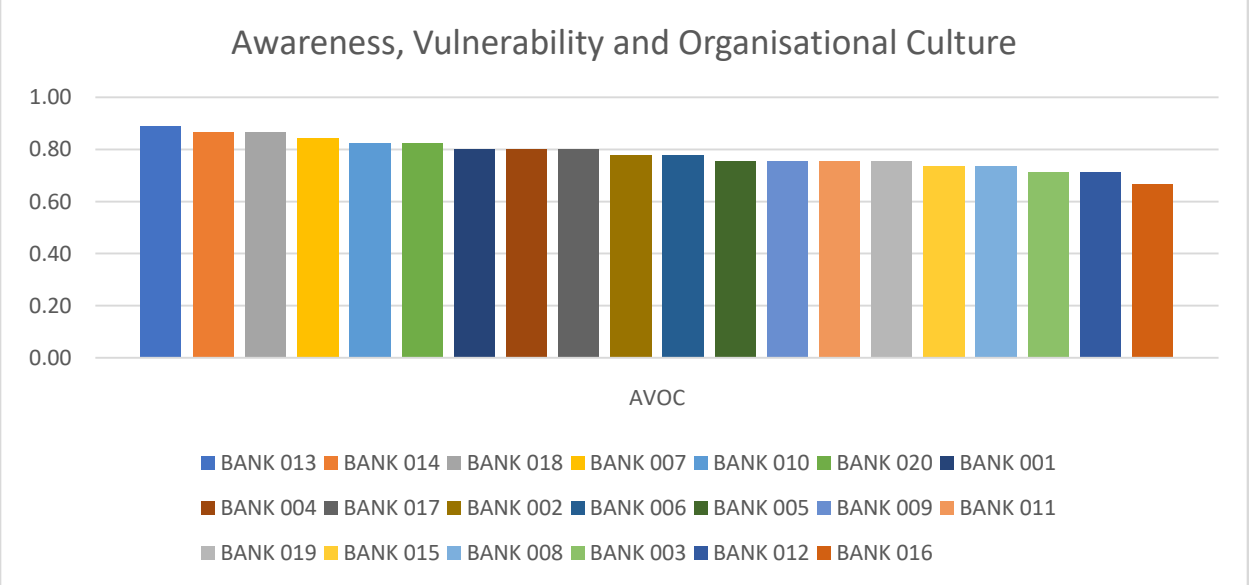


Figure 3: Awareness, Vulnerability and Organisational Culture

In Figure 3 is a graphical presentation of the data in Table 6. The data shows showed that banks employees have high awareness of the consequences of social engineering techniques, also agreeing that financial institutions are more prone to social engineering attacks while also

agreeing that employee behaviour and organisational culture have a role to play in improving the susceptibility of financial institutions to social engineering techniques.

Table 7 is a presentation of the data derived from the computations of the impact of social engineering attacks on the financial services sector. The names of the financial services organisation from which data was collected are coded to anonymised them as agreed on ethical grounds during data collection. SEII is the overall impact of social engineering attack that is derived from the other sub-metrics, namely; PI, EFI and ETI, these sub-metrics also have their underlining metrics to a granular level where quantitative data is collected. These data are further refined and presented graphically in the following sections.

Table 7: Summary of Impact of SE Attack Computation

BankCode	PI	EFI	ETI	SEII
BANK 001	0.80	0.60	0.60	0.67
BANK 002	0.80	0.60	0.60	0.67
BANK 003	0.73	0.53	0.60	0.62
BANK 004	0.60	0.47	0.47	0.51
BANK 005	0.93	0.80	0.73	0.82
BANK 006	0.60	0.60	0.60	0.60
BANK 007	0.80	0.73	0.60	0.71
BANK 008	0.53	0.47	0.33	0.44
BANK 009	0.67	0.60	0.60	0.62
BANK 010	0.80	0.67	0.53	0.67
BANK 011	1.00	0.87	0.60	0.82
BANK 012	0.60	0.60	0.53	0.58
BANK 013	0.80	0.60	0.40	0.60
BANK 014	1.00	0.80	0.60	0.80
BANK 015	0.60	0.67	0.53	0.60
BANK 016	0.67	0.53	0.73	0.64
BANK 017	0.87	0.60	0.40	0.62
BANK 018	0.67	0.67	0.47	0.60
BANK 019	0.60	0.53	0.47	0.53
BANK 020	1.00	0.67	0.60	0.76

Data Analysis

Figure 4 represents the social engineering impact index (SEII), which is the overall computation of the impact of social engineering attacks on the financial services sector. The Figure 4 present and aggregation of the SEII, namely, PI, EFI and ETI. The data shows that 2 (10%) of the assessed banks are in the extremely high category of impact; 10 (50%) are in the high category having scored in the range of 0.61-0.81. The remaining 8 banks (40%) are in the moderate range. There is no bank in the low and minimal score line.

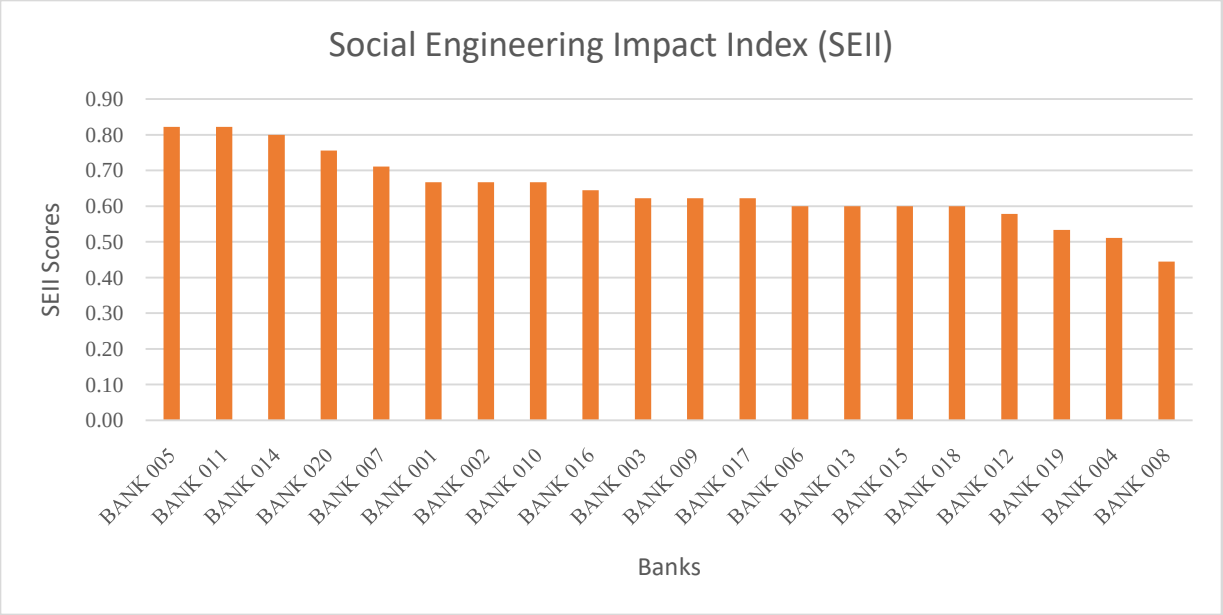


Figure 4: Social Engineering Impact Index (SEII)

Figure 5 is the privacy index (PI), it provides data on the impact of social engineering attacks on the privacy of customers with factors like identity, PFI and PII theft or compromise. The PI is one of the elements that forms the SEII earlier presented in Figure 3. The data in this Figure 5 shows that 5 (25%) of the assessed banks are in the extremely high category; 9 (45%) are in the high category and 6 (30%) are in the moderate category. Again, there is no bank that is impacted in the low and minimal categories.

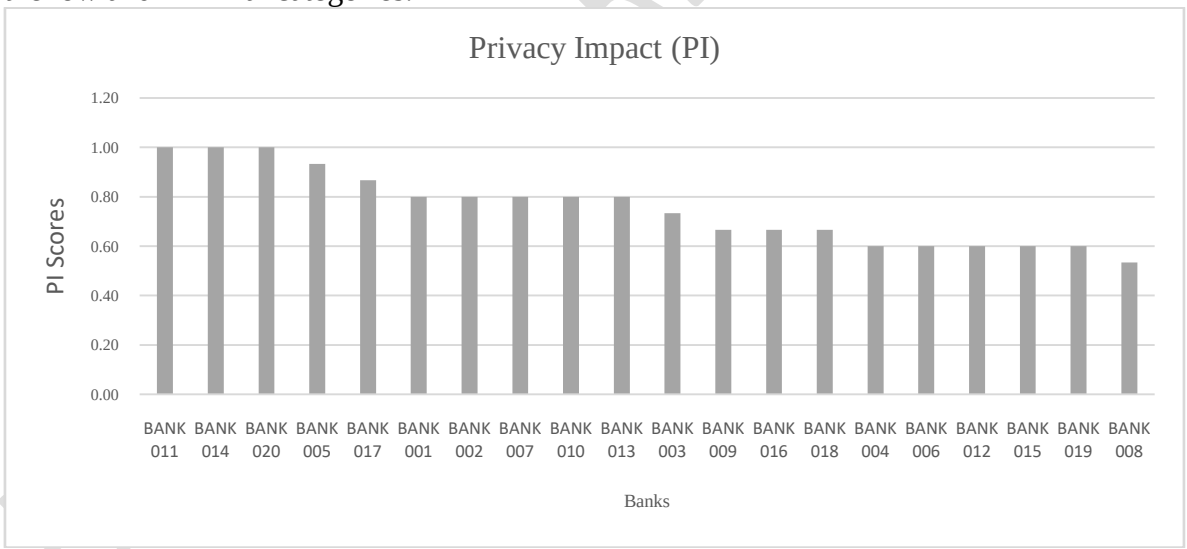


Figure 5: Privacy Impact

Figure 6 depicts the scores in the EFI, the date shows that 1 (5%) of the assessed institutions is in the extremely high category, 7 (35%) of them are in the high category while the remaining 12 (60%) are in the moderate position.

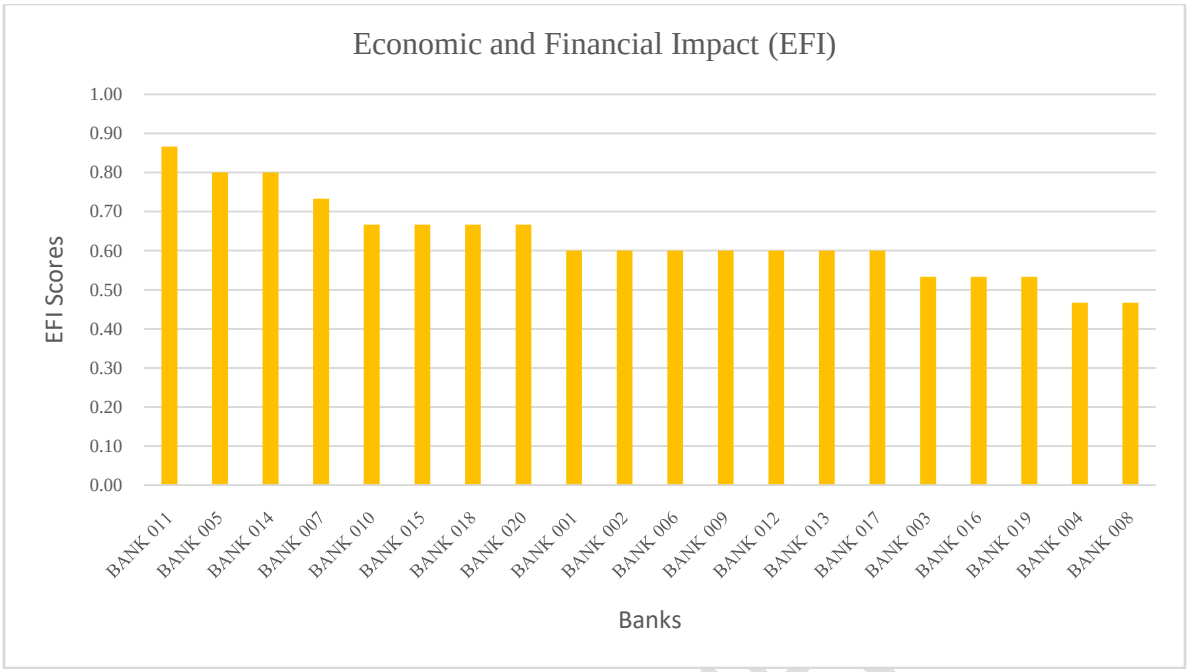
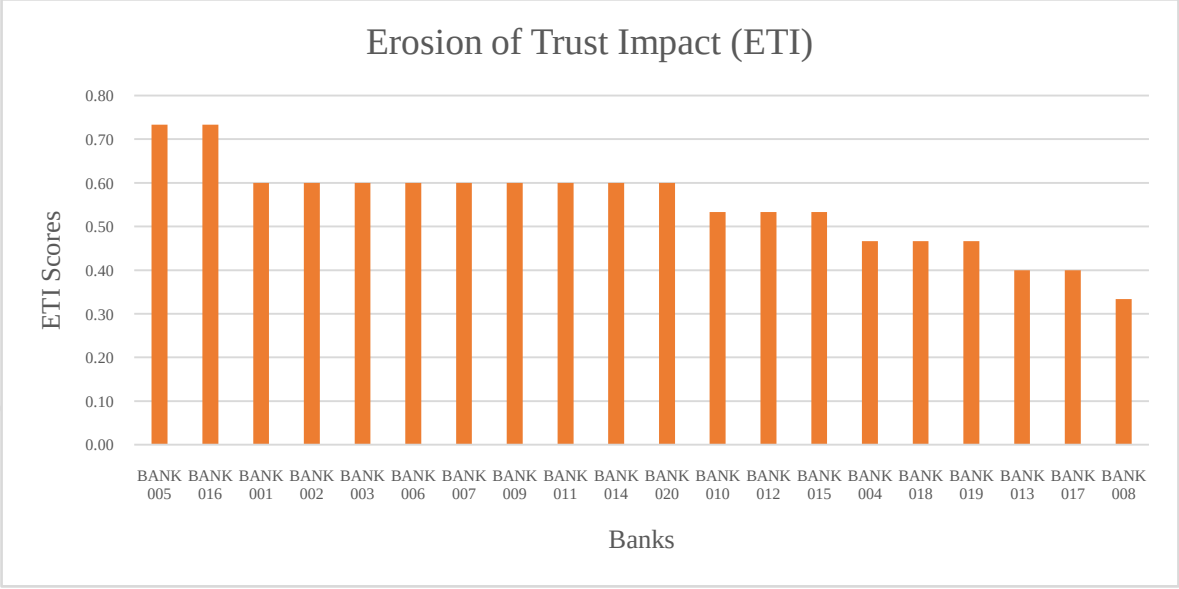


Figure 6: Economic and Financial Impact

Figure 7 is the ETI data which depicts the impact of social engineering attacks on trust within the affected financial institutions. The data showed that 11 (55%) of the assessed institutions are in high category, the remaining 9 (45%) are in the moderate category. There is no bank in the extremely high, low and minimal categories.



\

Figure 7: Erosion of Trust Impact

Comparison of Social Engineering Impact Factors (SEIF)

The social engineering factors provide lower-level measurements enable the understanding of the overall impact of social engineering attacks. The further understand the interplay in the results

displayed between Figures 4-7, Figure 8-10 attempts the compare the elements that makes up the privacy impact, economic and financial impact as well as erosion of trust impacts.

In Figure 8, it can be observed that PFI theft is the major target of the attackers as compared to PII and identity theft. The data shows that 7 (35%) of the organisation reported am extremely high PFI theft, 10 (50%) of the organisation reported high PFI theft. This is connected to the fact that social engineering attacks on bank customers or the banks are targeted at financial gains, accounting for the reasons the attackers are more concerned about the theft of PFI than they are concerned with victims identify and personally identifiable information. It must be noted that by this data, the PFI theft contributes the most to the high impact witnessed in PI SEI.

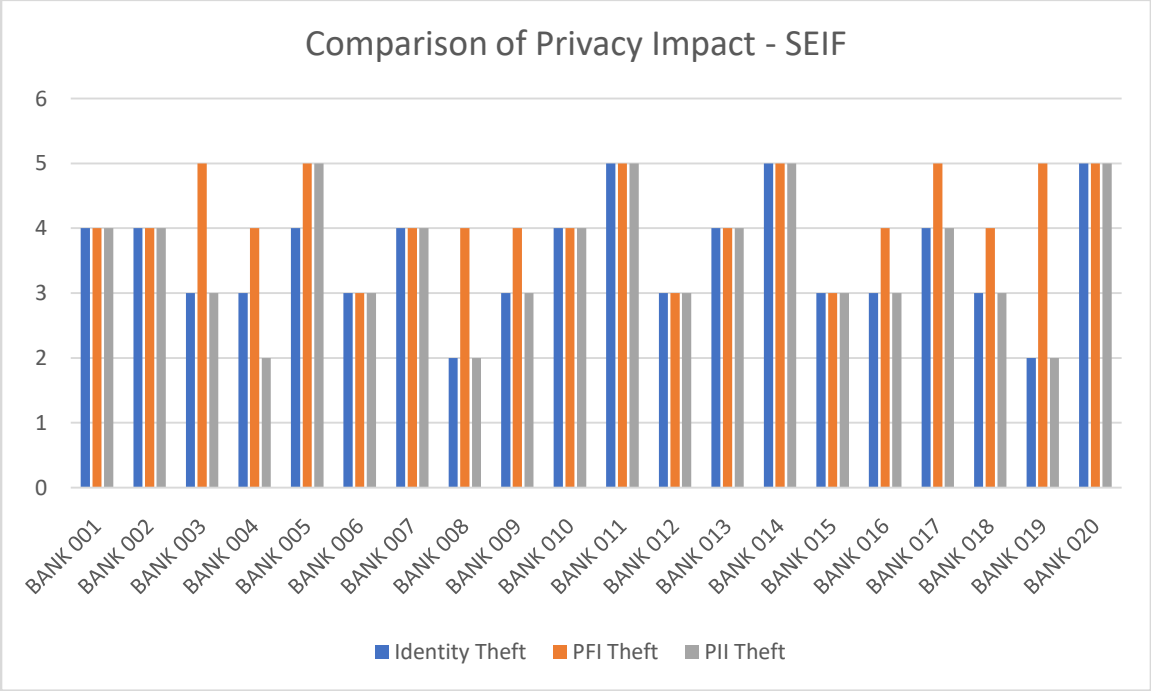


Figure 8: Comparison of Privacy Impact Social Engineering Impact Factors

Figure 8 presents the comparison of EFI factors, namely; success rate of social engineering attacks, amount stolen and number of customers affected. The amount stolen SEIF is the measuring contributor of impact on the EFI SEI, it has 2% extremely high and 40% high, it is followed closely by the success rate SEIF which has 40% high score. Majority of the number of customers affected SEIF are within the moderate (40%) score. This may be the fact that awareness has led to a reduction in the number of victims, however, the amount stolen and the success recorded is high.

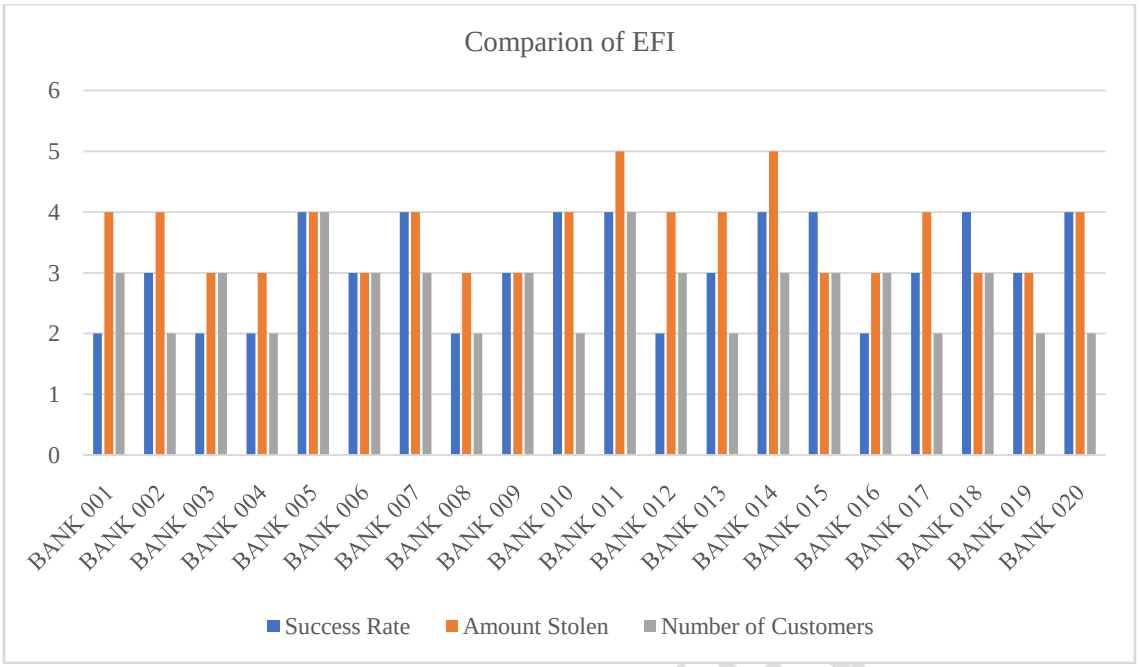


Figure 9: Comparison of Economic and Financial Impact Social Engineering Impact Factors

Figure 10 presents the comparison of ETI factors. The data in Figure 10 shows that service abandonment and damaged reputation are measure consequences suffered by the financial institutions during social engineering attacks.

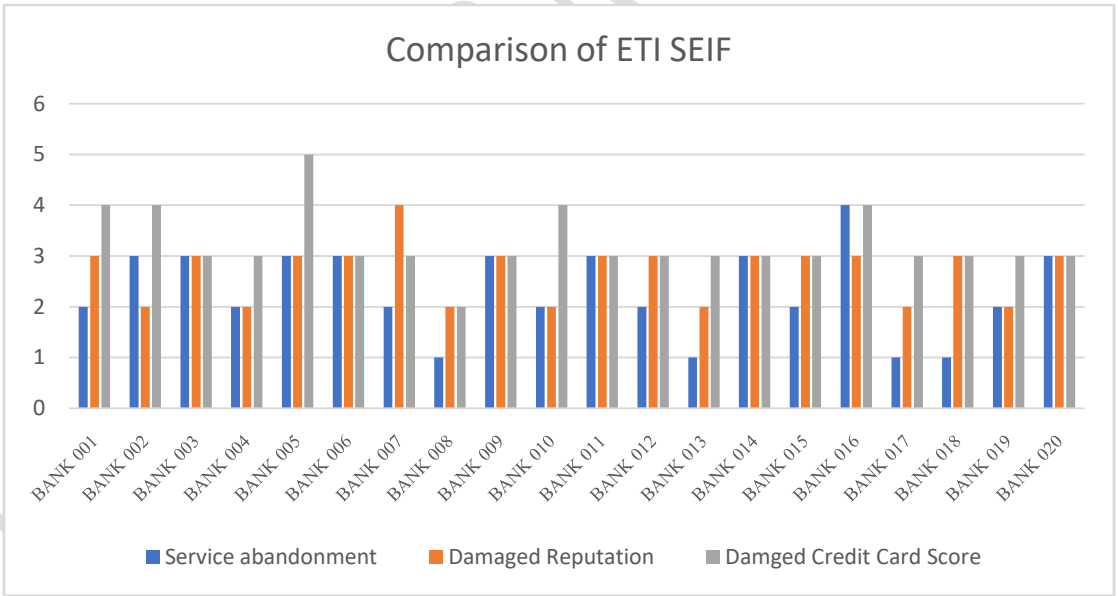


Figure 10: Figure 9: Comparison of Erosion of Trust Impact Social Engineering Impact Factors

Discussions and Conclusion

The aim of this study is to evaluate the impact of social engineering attacks in the financial sector. The import is to understand the extent of the consequences of social engineering attacks on the financial services sector. This data will support action by stakeholders to address social engineering attacks. To achieve this aim, at set of objectives were enumerated, thus, the findings

of this research will be evaluated against this research objectives. This will also show that the research questions were addressed.

Research Objective One*: To identify the factors responsible for social engineering attacks on the financial services sector.*

Determining the factors responsible for social engineering attacks in the banking services sector is crucial in the exercise of measuring the impact of social engineering attacks in the sector. Consequently, existing body of knowledge were explored to determine the factors that account for the most impact of social engineering attacks. Thus, from [1], [11], [12]and [32] privacy impact, economic and financial impact as well as erosion of trust impact were determined. Each of these have lower level impact account for their determination, namely; identity, PII and PFI theft for privacy impact; amount stolen, success rate and number of customers impacted for economic and financial impacts as well as service abandonment and damaged reputation for erosion of trust impact [4], [13] and [33]. These impacts as determined were presented in Figure 2.1 and used to derive the frameworks in Figures 4.1 and 4.2 respectively. This addressed research question one and achieved research objective one.

Research Objective two:*Determine how these factors can be measured to evaluate the impact of social engineering attacks on the financial services sector.*

Different methods, approaches and strategies were used based on the foundation of the pragmatic philosophical viewpoint [21] to formulate the social engineering impact assessment framework presented in Figure 4.1 and its extension in Figure 4.2. Based on these formulations, variables were defined and relationships established between and among them to support the derivation of the equations for the computation of the various impact indices, namely; the social engineering impact index (SEII), privacy impact (PI), economic and financial impact (EFI) and erosion of trust impact (ETI). This aspect accounted for the answering research question two and by extension achieving research objective two.

Research objective three: *To identify the metrics for quantifying the impact of social engineering attacks on the financial services sector.*

Based on the computation derived from the data against the computational models, the SEII which represented the social engineering impact index 10% of the organisations were in the extremely high category (i.e, they scored between 0.81-1.00), 50% are in the high category (scoring between 0.61-8.00) and 40% in the moderate category (0.41-0.60). There are no organisations scoring at the minimal and low categories. This data highlights the fact that the impact of social engineering attacks is generally high in the financial services sector.

A further analysis of the sub-metrics that made up the SEII reveals that on the PI metrics, 25% of organisations are in the extremely high category, 45% in the high category and 30% in the moderate category, again, there is no organisation in the low and minimal category, further underscoring the fact that the impact of social engineering attacks is generally high in the financial services sector. In the EFI, 5% - extremely high, 35% high and 60% medium. ETI reflects no organisation in the extremely high category, however, 55% of the organisation are in the high region and 45% in the medium region. It must be noted that in all the factors and subfactors considered, no organisation is impacted at the lower category.

Again, the research compared the social engineering impact factors (SEIF) of PI, EFI and ETI with their various sub-metrices. In the PI, the data showed that PFI theft is the most impact sub-metric, this is understandable due to the fact that the major motivation for social engineering attacks on the financial services sector is financial gain, and since personal financial information will provide access to the finances of the victims, they will be the most target and most stolen. Similarly, the amount stolen the is the highest contributing sub-metric in the economic and financial impact (EFI), this can be attributed to the fact that the driving force in this SE attacks is money [34]. In the ETI, the major contributor is the damaged credit card score. This data analysis and the findings that can be generated from the analysis answers research question three and by extension research objective three.

References

[1] Anderson, R., Moore, T., Bohme, R., & Clayton, R. (2012). Security economics and the economics of security. *Journal of Computer Security*, 20(3), 257-263.

[2] Hadnagy, C. (2011). Social Engineering: The Art of Human Hacking. *John Wiley & Sons*.

[3] Kaspersky Lab. (2015). *Carbanak APT: The Great Bank Robbery*. Retrieved from https://securelist.com/carbanak-apt-the-great-bank-robbery/68740/

[4] Federal Trade Commission. (2019). *Equifax Data Breach Settlement*. Retrieved from https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement

[5] Securities and Exchange Commission. (2020). SEC Charges Voya Financial Advisors With
Failing to Adopt Written Policies and Procedures Reasonably Designed to Protect Customer
Records and Information. Retrieved from https://www.sec.gov/news/press-release/2020-2

[6] NIST. (2021). *Cybersecurity Framework. National Institute of Standards and Technology*.

[7] Dhamija, R., Tygar, J. D., & Hearst, M. (2006, April 22). *Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in Computing Systems, 581-590.* Retrieved from https://doi.org/10.1145/1124772.1124861

[8] Blythe, J., & Rogerson, S. (2006). Pretexting: The art of deceit. . *International Journal of Electronic Security and Digital Forensics*, , 1(3), 303-312.

[9] Blythe, J., & Rogerson, S. (2006). Pretexting: The art of deceit. . *International Journal of Electronic Security and Digital Forensics*, , 1(3), 303-312.

[10] CrowdStrike. (2021). *2021 Global Threat Report. CrowdStrike Intelligence.*

[11] Ponemon Institute. (2020). *The 2020 Cost of Insider Threats: Global Report.* . Retrieved F rom https://www.observeit.com/resources/cost-of-insider-threats-report/.

[12] SolarWinds. (2021). *Threat Explainer: Supply Chain Attacks. SolarWinds Threat Explainer Series.*

[13] Baur, D. G., & Lucey, B. M. (2010). Is gold a hedge or a safe haven? An analysis of stocks, bonds and gold. *Financial Review*, 45(2), 217-229.

[14] Hijji, M., Alwan, K., & Al-Jabri, I. (2021). A multivocal literature review on growing social engineering threats during COVID-19. *Journal of Cybersecurity & Privacy*, 1(4), 1–22. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8545234/ PMC

[15] Washo, A. H., & Al-Najjar, B. (2021). An interdisciplinary view of social engineering: A call to research and practice. *Heliyon Interdisciplinary Security Review*, 2(1), 12–35. https://www.sciencedirect.com/science/article/pii/S2451958821000749ScienceDirect

[16] Accenture Security. (2021). *2021 Future cyber threats: Financial services* (Industry report). Accenture. https://www.accenture.com/_acnmedia/PDF-152/Accenture-2021-Future-Cyber-Threats-for-Financial-Services.pdf Accenture Banking Blog

[17] European Payments Council. (2021). *2021 Payments threats and fraud trends report*. EPC. https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2021-12/EPC193-21%20v1.0%202021%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdfEuropean Payments Council

[18] Cisco. (2021). *Security Outcomes Study — Financial services* (Report). Cisco Systems. https://www.cisco.com/c/dam/m/en_us/solutions/industries/financial-services/security-outcomes-study-fsi.pdfCisco

[19] Deloitte. (2021). *Future of cyber survey: Financial services insights* (White paper). Deloitte Touche Tohmatsu Limited. https://www.deloitte.com/global/en/services/consulting-risk/perspectives/gx-financial-services-cybersecurity-global-organizations.htmlDeloitte

[20] Nigeria Inter-Bank Settlement System (NIBSS). (2024). *2023 Annual Fraud Landscape* (Report). NIBSS. https://nibss-plc.com.ng/wp-content/uploads/2024/04/2023-Annual-Fraud-Landscape.pdfNIBSS

[21 Saunders, M., Lewis, P. and Thornhill, A. (2007). Research Methods for Business Students. 4th Edition, Financial Times Prentice Hall, Edinburgh Gate, Harlow.

[22] Mustapha, A., & Sinha, A. (2024). Cyberfraud in the Nigerian banking sector: Techniques and preventive measures. *SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4929630 SSRN

[23] Fast Payments / World Bank. (2023). *Fraud risks in fast payments* (Policy brief). World Bank / Fast Payments Taskforce. https://fastpayments.worldbank.org/sites/default/files/2023-10/Fraud%20in%20Fast%20Payments_Final.pdffastpayments.worldbank.org

[24] Chubb. (2024). *The impact of cyber scams on trust in digital payments: Digital payments trust report* (Industry report). Chubb. https://www.chubb.com/content/dam/chubb-sites/chubb-com/us-en/partnership/pdfs/digital-payments-trust-report.pdfChubb

[25] Doing, A. K., & Colleagues. (2024). An analysis of phishing reporting activity in a bank. *Proceedings of the ACM Conference on Financial Cybersecurity*, 1–11. https://dl.acm.org/doi/full/10.1145/3688459.3688481ACM Digital Library

[26] Oyewole, A. T., & Ibrahim, S. (2024). Cybersecurity risks in online banking: A detailed review of threats, impacts and mitigation. *Journal of Banking & Finance Security*, 8(2), 45–68. (PDF) https://pdfs.semanticscholar.org/da46/855de9412168081390efa0c34a626b40ef73.pdfSemantic Scholar PDFs

[27] Ahmed, F., & Khan, R. (2024). Digital risk and financial inclusion: Balancing protection and inclusion in digital banking. *Risks*, 12(8), Article 133. https://www.mdpi.com/2227-9091/12/8/133MDPI

[28] Laxman, V., & Colleagues. (2025). Emerging threats in digital payment and financial crime. *Journal of Financial Crime & Payments* (advance online). https://www.sciencedirect.com/science/article/pii/S2773067025000093ScienceDirect

[29] Andika, P. R. (2025). Fraud crime in banking using social engineering and trickery: Legal and regulatory perspectives. *Eduvest Journal of Finance & Law*, 3(1), 12–29. https://eduvest.greenvest.co.id/index.php/edv/article/download/50987/4400Eduvest

[30] Rathod, T., & Patel, S. (2025). A comprehensive survey on social engineering attacks and countermeasures. *Computers & Security Review* (in press). https://www.sciencedirect.com/science/article/abs/pii/S0306457324002875ScienceDirect

[31] Kalu, R. (2025). Investigation into online banking and its prevailing fraud factors. *Preprints* (open access preprint). https://www.preprints.org/manuscript/202503.1711/v1/downloadPreprints

[32] Akibeer, H. J. (2025). The evolution of social engineering attacks: Trends and implications for financial services. *Regional Journal of Emerging Security*, 6(1), 77–98. https://rjes.iq/index.php/rjes/article/view/166Rafidain Journal

[33] Hijji, M., & Colleagues. (2022). Social engineering techniques during pandemics: lessons for banks and financial institutions. *International Journal of Information Security Studies*, 9(3), 101–120. (See multivocal review discussion). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8545234/ PMC

[34] Financial Times. (2024, July 23). Technology and cyber crime: How to keep out the bad guys (analysis). *Financial Times*. https://www.ft.com/content/8a79ab25-c902-4110-bcb8-be2fd422f6bfFinancial Times