ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14928696

# Psychological Tactics of Social Engineering in Nigeria: A Study of Vulnerability Patterns and Countermeasures in the Digital Age

Oraka Chinelo Judith

Department of Computer Science, University of Nigeria Nsukka

Publication Date: 2025/02/26

**Abstract: Social engineering has evolved into a significant threat to cybersecurity in Nigeria as it preys on human vulnerabilities to breach entry into sensitive information. This paper explores the psychological techniques used by social engineers, such as phishing, pretexting, baiting, and urgency tactics and goes further to analyze socio-economic and cultural factors aggravating the tendency to such attacks from the Nigerian perspective. It underscores the vital role that cognitive biases, such as authority bias and reciprocity, play in shaping victim behavior. The paper also discusses vulnerability patterns of low digital literacy, high trust in authority and economic pressures that make citizens and organizations prime targets for cybercriminals. In addition, it discusses very comprehensive countermeasures including public education, stronger authentication protocols, policy enforcement, technological innovations, and grassroots solutions, which are tailored to Nigeria's unique contexts. Thus, it focuses on suppressing or combating these vulnerabilities through a multi-pronged strategy ensuring a collaboration between government, private organizations, and civil society towards building a sustainable digital ecosystem. In this way, this study contributes to the bigger discourse on cybersecurity in developing countries. The study also probated action research into how people in a developing country such as Nigeria can go beyond social engineering threats.**

*Keywords: Social Engineering; Psychological Tactics; Cybersecurity; Phishing; Vulnerability; Countermeasures.*

**How to Cite:** Oraka Chinelo Judith (2025) Psychological Tactics of Social Engineering in Nigeria: A Study of Vulnerability Patterns and Countermeasures in the Digital Age. *International Journal of Innovative Science and Research Technology*, 10(2), 607-613. https://doi.org/10.5281/zenodo.14928696

## I. INTRODUCTION

The rise of the digital economy has introduced immense opportunities for economic growth, innovation, and connectivity. Nigeria, as Africa's largest economy and most populous country, has experienced rapid digital transformation, driven by increasing internet penetration and the adoption of mobile technologies (Bosun, 2024). According to the Nigerian Communications Commission (NCC), internet penetration in the country surpassed 45% in 2022, providing access to millions of people (NCC, 2022). While this expansion has fueled economic growth, it has also created vulnerabilities to cyber threats, particularly social engineering attacks.

Social engineering, as defined by Schneier (2015), is the psychological manipulation of individuals to perform actions or divulge confidential information. Unlike conventional hacking that focuses on technical exploits, social engineering exploits human psychology and behavior. This makes it an effective and dangerous tool for cybercriminals, as even the most secure technological systems remain vulnerable to human error.

Specific contextual factors beyond the heightened prevalence of social engineering in Nigeria are issues such as low levels of digital literacy, weak cybersecurity infrastructure, and socioeconomic challenges to which the people are vulnerable. For example, high unemployment levels with deep-rooted poverty often cause people to fall into scams of getting rich quickly, heavily dependent on social engineering tactics (Olowu, 2021). In addition, cultural norms like the ones that emphasize trust and respect for authority make the potential ground fertile for exploitation by social engineers.

In this study, we examine the psychological techniques of social engineering in Nigeria, point out key vulnerable patterns, and identify their causes. We would also suggest some interventions to combat these threats, including digital education, awareness campaigns, and cyber security frameworks. The research is intended to offer valuable insight

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14928696

into these issues with the long-term objective of making Nigeria a safer and more secure nation technologically.

## II. THE PSYCHOLOGICAL TACTICS OF SOCIAL ENGINEERING

Social engineering thrives on exploiting human psychology rather than technical vulnerabilities. Cybercriminals use various psychological tactics, manipulating cognitive biases, emotions, and trust to deceive their targets. These tactics exploit fundamental aspects of human behavior, such as the tendency to trust authority, act under pressure, or desire rewards (Kumar & Tiwari, 2024). Below are the most prevalent tactics of social engineering and how they are applied in Nigeria:

➢ *Phishing*

Phishing is the most prevalent form of social engineering, exploiting human trust to steal highly sensitive information. It usually is channeled through emails, messages, or websites designed to appear legitimate. In Nigeria, phishing attacks have recorded increases because of the increased adoption of digital platforms for banking, communication, and commerce (Zainab Alkhalil et al., 2021). For example, individuals, businesses, and government agencies, among others, are targeted by cybercriminals using these attacks to leverage the many bottlenecks in the country, such as low digital literacy, socio-economics, and inadequate cybersecurity awareness.

Phishing typically involves spoofing trusted entities, such as banks or government agencies, or popular service providers to extract sensitive information from victims, including passwords and financial or identification numbers (Kosinski, 2024). A widespread phishing approach that exists in Nigeria involves sending fraudulent emails or SMS claiming to come from the Central Bank of Nigeria (CBN) or any commercial bank. These usually warn the target of some account problems or breaches of security and instruct them to click a link or enter account credentials immediately (Kaushik et al., 2021).

## III. CASE ANALYSIS: PHISHING ATTACK IN NIGERIA

In 2020, a major phishing action-affecting customer of one of the largest telecommunications providers in Nigeria was recorded. The perpetrators sent messages that claimed to be from the telecommunications company and that the users should take action to avoid their accounts being deactivated by verifying their identity over some link provided (Punch, 2020). When clicked, the link redirected the hapless victims to a fake login page imitating that of the company so that they could unknowingly fill in their details. The outcome was unauthorized entry into the victims' mobile wallets and potential monetary theft.

The attack was successful due to many reasons such as:

- High Trust in Known Entities: The victim uses the branding and language of the company to believe that the message is legit.
- Urgency: The message sought an immediate decision and panic, thus lessening the chance for surfing.
- Low Digital Literacy: Many victims thus do not have the skills to recognize the URL as fake or the website as fake.

The attack emphasizes how phishing schemes exploit a combination of trust and urgency to trick their victims, often in ways that cause them huge financial loss and psychological trauma (Abiola Odutola, 2020).

Phishing is mainly harbored in Nigeria by the socio-economic environment. For example, job phishing or grant phishing usually targets unemployed individuals. Scammers often pose as famous organizations in sending emails or messages that may require personal details or upfront payment for processing fees (Thompson et al., 2020). Given the fact that it is a struggling economy, the promise of financial relief lures many especially those in a desperate situation.

Additionally, phishing attacks targeting rural communities have surged as mobile banking services expand to underserved areas (Ashiru, 2021). Many individuals in these regions are first-time digital users with limited understanding of secure online practices, making them prime targets.

➢ *Pretexting*

Pretexting is a very advanced form of social engineering whereby the attackers create and invent some false scenario or "pretext" to fool the victim into giving confidential information or doing something else for the criminal (SentinelOne, 2024). Unlike phishing, which has a wide net catchall, pretexting has become very specialized and personalized tactics that leverage trust, authority, and relationships for the fraud. Nigeria is where pretexting is one of the most effective forms for cyber-criminals, and that has a lot to do with how people have high trust in authority figures and institutions (UMATechnology, 2024).

Pretexting typically involves extensive research on the target. The attacker gathers details about the victim—such as their job role, organization, family, or personal interests—using publicly available information or prior breaches. Armed with this knowledge, they create a believable narrative to approach the victim (Fruhlinger, 2020). Common examples in Nigeria include:

- Impersonation of Authority Figures: Attackers pose as representatives of banks, government agencies, or utility companies, requesting sensitive information under the guise of resolving a problem.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14928696

- Business Email Compromise (BEC): Criminals impersonate senior executives to instruct employees to perform unauthorized transactions or share confidential data (Fruhlinger, 2020).
- Socially Driven Pretexting: Attackers pose as relatives or close friends needing urgent financial help, leveraging communal and familial bonds to exploit their targets.

## IV. CASE ANALYSIS: PRETEXTING IN NIGERIA

➢ *Case 1: Business Email Compromise*

In 2019, a Nigerian company went under attack due to pretext. An employee received an urgent email from his boss impersonating the CEO. The message issued instructions to send some funds immediately to the supplier for a critical business need (Renals, 2021). The employee performed the transaction thinking it was a genuine email-in-doing so leading to the loss of several million naira. The name, title, and style of writing were all true to the individual whose name was used, thereby making it appear real as the attacker had thoroughly studied the individual at some points from public social media posts and email leaks.

➢ *Case 2: Fake SIM Registration Requests*

Pretexting scams also leverage Nigeria's ongoing SIM registration and revalidation efforts. Attackers pose as telecom operators, contacting victims and claiming their SIM cards will be deactivated unless they provide their National Identification Number (NIN) or other personal details (Nation, 2019). The sense of urgency and perceived legitimacy of these requests often leads victims to comply, exposing them to identity theft and financial fraud.

## V. PSYCHOLOGICAL TACTICS IN PRETEXTING

Pretexting relies on several psychological principles to deceive victims (Meta-Techs, 2024):

- Authority and Trust: People are more likely to comply with requests from perceived authority figures, such as bank officials or company executives.
- Urgency: Creating a sense of time pressure prevents victims from carefully scrutinizing the request.
- Personalization: Tailoring the pretext to the victim's specific context, such as referencing recent events or known associates, makes the request more convincing (Meta-Techs, 2024).

In Nigeria's collectivist culture, where social bonds and trust in authority are highly valued, these tactics become even more effective.

➢ *Baiting*

Consequently, baiting is a social engineering tactic that capitalizes on the tendencies of humans, especially curiosity or avarice, thereby presenting lures for victims (Cybrvault, 2024). Baiting schemes in Nigeria usually take the shape of fake job offers, free data bundles, or promotional giveaways that lure victims into disclosing their personal details such as banking credentials or National Identification Numbers (NINs). The most typical example of baiting is leaving a malicious flash drive labeled "confidential" or "important" in public places and when it is plugged into a computer it can install some malware (Izuakor, 2021). One more example of baiting is the online scheme whereby victims are directed to another fake website to claim their prize. The success of baiting lies in its aptitude to prey on the curiosity and socio-economic wants of the individuals; an especially viable target is therefore low-income settings where free offers become enticing (Rudra, 2024). Ways of fighting baiting include public awareness campaigns that focus on building skepticism about unsolicited offers and the practice of safe behavior in the digital world like link verification and avoiding unknown devices.

➢ *Quid Pro Quo*

In a quid pro quo attack, social engineers offer a service or benefit in return for information. For instance, they may claim to assist with recovering lost accounts but require the victim's credentials to do so. This tactic is particularly effective in Nigeria's informal economy, where trust-based exchanges are common, and individuals often seek quick solutions to technological issues (Nigerian Communications Commission, 2022).

➢ *Urgency and Fear*

Drumming urgency and fear is one of the best ways to push a victim into making quick decisions. A social engineer may send a message to an individual saying that his bank account will be blocked unless he does something quickly, and thus will urge the victim to give sensitive information. Fear tactics are especially useful in Nigeria, as many people trust financial institutions but don't understand them (Olowu, 2021).

➢ *Exploitation of Social Norms*

In Nigeria, societal norms such as respect for authority, social engineers often exploit communal sharing, and familial obligations. For example, attackers may impersonate relatives in need of financial assistance or community leaders requesting donations for a cause. These schemes rely on emotional manipulation and the cultural emphasis on helping others (David & Bode-Asa, 2023).

➢ *Cognitive Biases and Social Engineering*

The success of social engineering attacks is rooted in their exploitation of well-known, well-studied cognitive biases. These include:

- Authority bias: The victims become more amenable to the solicitation coming from people considered to have authority such as bank officials.
- Reciprocity Bias: The principle of the tendency to feel obliged to pay back favors, being exploited in quid pro quo schemes.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14928696

- Overconfidence Bias: Individuals usually exaggerate their ability to detect fraud and therefore do not take precautions when interfacing with the potential attacker (Schneier, 2015).

Such tactics call for a more intellectual appreciation of psychological manipulation within the culture of Nigeria, where many of the economic-cultural and educational influences have created inbuilt peculiar vulnerabilities.

➢ *Vulnerability Patterns in Nigeria*

Nigeria's unique socio-economic, cultural, and technological landscape has created specific vulnerabilities to social engineering attacks. These patterns stem from structural challenges, individual behaviors, and cultural norms that attackers exploit (Nwegbu et al., 2015). Below is an in-depth analysis of the major vulnerability patterns and the underlying factors that contribute to them.

➢ *Low Digital Literacy*

One of the primary drivers of susceptibility to social engineering in Nigeria is the low level of digital literacy among the general population. Despite increased internet penetration, many Nigerians lack basic knowledge of cybersecurity best practices. For example, a significant portion of users cannot distinguish between legitimate websites and phishing sites, making them easy targets for cybercriminals (Nigerian Communications Commission, 2022).

Digital illiteracy is particularly prevalent in rural areas, where access to formal education and exposure to technology are limited. This gap is exploited by attackers who create schemes targeting individuals unfamiliar with secure online behavior. Studies indicate that phishing emails and SMS messages claiming to be from trusted institutions often succeed because victims fail to verify their authenticity (Aborisade & Adesanya, 2020).

➢ *High Trust in Authority Figures*

The cultural influences present within Nigeria encourage respect for authorities or authority figures, thus making compliance with requests an involuntary act. Social engineers impersonate officials who are always from either banks, governmental agencies, or police departments to steal sensitive information from potential victims. An example would be the attackers pretending to be representatives from the Central Bank of Nigeria (CBN) to extract trust and access financial details from their victims (Olowu, 2021).

Such levels of trust take much advantage of "pretexting," where victims relay personally or corporately originated information believing it to be legitimate. Indeed, many institutions have poor customer support structures, which also compound the problem of making verifications on such claims difficult for potential victims.

➢ *Socioeconomic Pressures*

Economic challenges such as high unemployment, inflation, and poverty make Nigerians particularly vulnerable to financial fraud schemes. Social engineers exploit this vulnerability through "get-rich-quick" scams, fake investment opportunities, and lottery fraud. According to the Nigerian Cybercrime Report (2022), fraudulent schemes promising large financial rewards are among the most successful forms of social engineering in Nigeria.

Many victims fall for these schemes because of the allure of escaping economic hardship. Cybercriminals craft compelling narratives that tap into the aspirations of financially strained individuals, convincing them to part with their money or sensitive information (Aborisade & Adesanya, 2020).

➢ *Cultural Norms and Collectivism*

Nigerian society is fundamentally collectivistic, valuing communalism, as well as family, and mutual support. This would have brought in solid community ties but would also include vulnerabilities that social engineers can use for exploitation (Asawo & Blue-Jack, 2016). For example:

- Familial Trust: Attackers impersonate family members in distress, requesting urgent financial assistance.
- Communal Obligations: Fraudsters often pose as community leaders or members, soliciting donations for fabricated causes.

Such tactics leverage the societal expectation to help others, especially during any such perceived crises (Olowu, 2021). Citizens in this kind of environment would not pay close attention to such requests ostensibly because of the emotional and cultural pressure to act.

## VI. OVERRELIANCE ON MOBILE TECHNOLOGY

Increased convenience made available by mobile phones and digital payment systems opens up the attack surface for cybercriminals. Mobile users are inundated with messages (smishing) and unremittingly fraudulent calls. Failure to adopt secured ways of communicating, such as verifying unsolicited messages, has added momentum to these attacks (Nigerian Communications Commission, 2022).

For instance, they may tell users to send the message as if it is coming from their mobile network provider and require them to divulge their personal identification numbers (PINs) or any other sensitive information. This is followed by the high penetration of mobile money services, MTN's MoMo in particular, which augments the chances of being at risk of social engineering regarding financial fraud.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14928696

➢ *Weak Cybersecurity Infrastructure*

The cybersecurity environment in Nigeria is quite immature and leaves individuals and organizations exposed to attack. Many businesses have not yet equipped themselves with all the necessary tools for defense against social engineering such as firewalls, endpoint security solutions, and employee training programs. More so, the absence of a strong cybersecurity culture at both individual and organizational levels stretches this vulnerability (Nigerian Cybercrime Report, 2022).

There is a lack of enforcement and ineffectiveness in cybersecurity laws like Cybercrime (Prohibition, Prevention, etc.) Act, 2015. Such absence of deterrence gives audacity to cybercriminals to the scheme using social engineering means without keener fear of penalties.

➢ *Countermeasures against Social Engineering*

Human vulnerability continues to be exploited by social engineering. Countermeasures have become inevitable because of the rapid digitalization of the economy in Nigeria. These countermeasures must also be applied at the root level of susceptibility bringing forward both individual behavior and systemic weakness. (Li et al. 2023). Below are the countermeasures elaborated in detail with special emphasis on the relevance of these countermeasures in the Nigerian context.

➢ *Awareness Campaigns*

Public awareness is one of the most effective defenses against social engineering. Education programs aimed at demystifying cyber threats and teaching safe online behaviors are essential (Quinlan, 2020). In Nigeria, such campaigns should focus on:

- Digital Hygiene: Teaching individuals to recognize phishing attempts, verify requests, and avoid sharing sensitive information online.
- Localized Messaging: Using local languages and culturally relevant examples to ensure the message resonates with diverse demographics.

For example, awareness programs run by organizations like the Nigerian Communications Commission (NCC) and CyberSafe Foundation have successfully reached urban and rural populations, reducing the impact of phishing attacks (CyberSafe Foundation, 2021).

➢ *Cybersecurity Training Programs*

Organizations must prioritize employee training on cybersecurity. Since human error is often the weakest link in security frameworks, equipping individuals with the knowledge to detect and mitigate social engineering attempts is crucial (Rathod et al., 2024). In the Nigerian context:

- Mandatory Corporate Training: Companies should integrate cybersecurity modules into their onboarding processes. Training should include simulated phishing attacks to help employees recognize and respond to threats effectively.
- Sector-**Specific Programs**: Industries like finance, healthcare, and education, which handle sensitive information, require tailored training programs to address unique risks (Aborisade & Adesanya, 2020).

➢ *Stronger Authentication Protocols*

Advanced authentication methods can effectively make threats from social engineering quite rare, as these would ensure that only authorized users gain access due to the sensitive nature of the system or data (Rathod et al. 2024). Recommended practice includes:

- Multi-Factor Authentication MFA: It combines something that the user knows (some password), something they have (like a smartphone), and something they are (biometrics).
- Behavioral Biometrics: Implement tools that establish the different patterns of typing or mouse movements or which establish the login times to identify unusual behavior.

In Nigeria, many banks such as Access Bank and GTBank have already implemented this scheme into their systems to protect online banking platforms, relatively reducing the number of fraud cases (Nigerian Cybercrime Report 2022).

➢ *Policy Implementation and Enforcement*

Government policies and regulatory frameworks play an important role in combating social engineering. Nigeria has gained from the enactment of the Cybercrime Prohibition, Prevention, Etc. Act of 2015, but enforcement remains a real problem. To strengthen the effectiveness:

- Stronger Penalties for Cybercriminals: Making social engineering and other cybercrimes much harsher with legal consequences could dissuade prospective victims.
- Public-Private Partnerships: Collaborations between government and private companies as well as international organizations could foster infrastructure development in the country concerning cybersecurity.
- Real-Time Reporting Platforms for Incidents: Central platform vicinity for individuals and organizations to report suspected scams or breaches (Cybercrime Act, 2015).

➢ *Technological Tools and AI Integration*

Technology-driven solutions are used in recognizing and addressing social engineering attempts. These include:

- Artificial Intelligence detection: Analyze communication patterns by leveraging artificial intelligence to highlight anomalies and detect phishing attempts.
- Anti-Phishing Software: Install software that prohibits access to known malicious websites and raises real-time alerts.
- Insecure communication channels: Encourage the use of encrypted messaging applications that protect sensitive information (Schneier, 2015).

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14928696

➢ *Community-Driven Solutions*

Given Nigeria's collectivist culture, community-based approaches can be highly effective. For example:

- Cybersecurity Ambassadors: Training influential members of communities to serve as cybersecurity educators and advocates.
- Local Helplines: Establishing toll-free numbers where individuals can verify suspicious requests or report scams.

➢ *Targeted Interventions for Vulnerable Groups*

Some communities like small business owners, the elderly, and rural people face various social engineering attacks. Following are some such interventions:

- Workshop for SMEs: Small businesses usually do not have proper cybersecurity. Workshops may impart specific skills and essential tools for protecting their work.
- Digital Literacy for Seniors: Programs emphasize access to specific technologies for older adults to help them navigate their use safely.
- Rural Outreach Programs: Expanding the border of access to cybersecurity education into less accessible areas and utilizing mobile technology and radio broadcasts (Olowu, 2021).

## VII. CONCLUSION

Dangerous social engineering attacks are now posing threats to the digital ecosystems of Nigeria, exploiting psychological weaknesses, socioeconomic coercions, and cultural leanings. The fact that these attacks are realizable simple has a lot to do with the current economic realities where people are highly persuadable with scant digital literacy and high faith in authority. Addressing such vulnerabilities would require a full-scale and multi-pronged strategy in the form of a public education drive to fill the digital literacy gap for Nigeria's various populations. Initiatives like these should better equip the public to identify and deflect cyber threats. This would also strengthen enforcement of existing laws like Cybercrime (Prohibition, Prevention, etc.) Act and new laws to send a clear message to cybercriminals. Technology solutions will also include multi-factor authentication, AI detection, and secure digital platforms, among others, to mitigate risks. Community-based projects with cybersecurity ambassadors and local support networks can use Nigeria's collectivist culture effectively to foster a sense of shared responsibility for online safety. To ensure the inclusiveness of solutions, however, extra care needs to be taken regarding disadvantaged groups, including small businesses and rural areas. These initiatives will largely depend on public-private partnerships as well as civil society. With education technology policy and community participation, Nigeria will be able to strengthen its defenses against social engineering attacks and future-proof its digital future while setting an example for other developing countries.

## REFERENCES

[1]. Aborisade, O. P., & Adesanya, O. (2020). Cybercrime in Nigeria: Trends and implications. Journal of Cybersecurity Studies, 5(2), 45–56.

[2]. Asawo, S. P., & Blue-Jack, A. I. (2016). Collectivism and Organizational Success: Managing Cultural Diversity in Nigeria's Multicultural Corporations for National Development. ResearchGate. https://www.researchgate.net/publication/308968550_Collectivism_and_Organizational_Success_Managing_Cultural_Diversity_in_Nigeria's_Multicultural_Corporations_for_National_Development

[3]. Ashiru, A. (2021). Identifying Phishing as a form of Cybercrime in Nigeria: Interrogating the Laws and Exposing the Evil. ResearchGate. https://doi.org/10211258/Number-of-phishing-URLs-Q3-2013-to-Q1-2021_Q320

[4]. Bosun Tijani. (2024, September 18). Nigeria seeks digital transformation for a stronger economy. World Economic Forum. https://www.weforum.org/stories/2024/09/nigeria-digital-transformation-3mtt-technical-talent/

[5]. CyberSafe Foundation. (2021). State of cybersecurity awareness in Nigeria: Annual report. Retrieved from https://cybersafefoundation.org

[6]. Cybrvault. (2024, December 23). What is Baiting in Cyber Security? Cybrvault. https://www.cybrvault.com/post/what-is-baiting-in-cyber-security

[7]. David, U., & Bode-Asa, A. (2023). An Overview of Social Engineering: The Role of Cognitive Biases Towards Social Engineering-Based Cyber-Attacks, Impacts and Countermeasures. ResearchGate. https://doi.org/10.13140/RG.2.2.12421.12003

[8]. Fruhlinger, J. (2020, June 4). What is pretexting? Definition, examples, and attacks. CSO Online. https://www.csoonline.com/article/569453/what-is-pretexting-definition-examples-and-prevention.html

[9]. Izuakor, C. F. (2021). Cyberfraud: A Review of the Internet and Anonymity in the Nigerian Context. ResearchGate. https://www.researchgate.net/publication/350941930_Cyberfraud_A_Review_of_the_Internet_and_Anonymity_in_the_Nigerian_Context

[10]. Kaushik, K., Singh, S., Garg, S., Singhal, S., & Pandey, S. (2021). Exploring the mechanisms of phishing. Computer Fraud & Security, 2021(11), 14–19. https://doi.org/10.1016/s1361-3723(21)00118-4

[11]. Kosinski, M. (2024, May 17). Phishing. Ibm.com. https://www.ibm.com/think/topics/phishing

[12]. Kumar, R., & Tiwari, Dr. Shikha. (2024). Social Engineering: Its Significance and Implications for Future Research. International Journal of Research Publication

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14928696

and Reviews, 5(1), 4255–4263. https://doi.org/10.55248/gengpi.5.0124.0324
[13]. Li, T., Song, C., & Pang, Q. (2023). Defending against social engineering attacks: A security pattern-based analysis framework. IET Information Security, 17(4), 703–726. https://doi.org/10.1049/ise2.12125
[14]. Meta-Techs. (2024). Meta-Techs.net. https://meta-techs.net/pretexting-in-cyber-security/
[15]. Nation, T. (2019). Confronting dangers of pre-registered SIM cards - The Nation Newspaper. The Nation Newspaper. https://doi.org/10/12140214/cropped-nation-cropped-l-32x32
[16]. Nigerian Communications Commission. (2022). Internet penetration and cybersecurity in Nigeria. Retrieved from https://www.ncc.gov.ng
[17]. Nigerian Cybercrime Report. (2022). Annual report on cybercrime in Nigeria. Retrieved from https://www.nigeriancybersecurity.org
[18]. Nwegbu, M., Eze, C., & Asogwa, B. E. (2015). Globalization of Cultural Heritage: Issues, Impacts, and Inevitable Challenges for Nigeria. ResearchGate. https://www.researchgate.net/publication/265241456_Globalization_of_Cultural_Heritage_Issues_Impacts_and_Inevitable_Challenges_for_Nigeria
[19]. Olowu, A. Y. (2021). Psychological implications of cybersecurity in Nigeria. African Journal of Psychology, 18(3), 92–105.
[20]. Punch. (2020). Punchng.com. https://punchng.com/how-nigeria-us-19-others-lost-over-4-1b-to-cyber-fraud-business-scam-in-2020-fbi/
[21]. Quinlan, L. (2020). A Solution for Human Vulnerabilities to Social Engineering Attacks: The Social Engineering Defence Model. ResearchGate. https://doi.org/10.13140/RG.2.2.35328.66562
[22]. Rathod, T., Jadav, N. K., Sudeep Tanwar, Abdulatif Alabdulatif, Garg, D., & Singh, A. (2024). A comprehensive survey on social engineering attacks, countermeasures, case study, and research challenges. Information Processing & Management, 62(1), 103928–103928. https://doi.org/10.1016/j.ipm.2024.103928
[23]. Renals, P. (2021, October 7). SilverTerrier – Nigerian Business Email Compromise. Unit 42. https://unit42.paloaltonetworks.com/silverterrier-nigerian-business-email-compromise/
[24]. Rudra, A. (2024, February 25). PowerDMARC. PowerDMARC. https://powerdmarc.com/what-is-a-baiting-attack/
[25]. Schneier, B. (2015). Data and Goliath: The hidden battles to collect your data and control your world. New York: W. W. Norton & Company.
[26]. SentinelOne. (2024, December 11). What is Pretexting? Attacks, Examples & Techniques. SentinelOne. https://www.sentinelone.com/cybersecurity-101/cybersecurity/pretexting/
[27]. The Cybercrime (Prohibition, Prevention, Etc.) Act. (2015). Official Gazette of Nigeria. Retrieved from https://www.lawsofnigeria.org
[28]. Thompson, J., Adebayo, I. A., & Emmanuel, E. (2020). Cybercrime and Socio-economic Development of Corporate Organizations in Cross River State, Nigeria. Asian Journal of Scientific Research, 13(3), 205–213. https://doi.org/10.3923/ajsr.2020.205.213
[29]. UMATechnology. (2024, December 24). What Is a Pretexting Attack and How Can You Protect Yourself? - UMA Technology. UMA Technology. https://umatechnology.org/what-is-a-pretexting-attack-and-how-can-you-protect-yourself/
[30]. Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf, & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Frontiers in Computer Science, 3. https://doi.org/10.3389/fcomp.2021.563060