Journal of Development and Society, Faculty of Social Sciences, University of Abuja
Vol.7.3, 2026 https://uniabujafsos.com.ng/ ISSN:0331-000 Special Issue

Cyber Security Awareness and Social Media Behavior among Nigerian Youths: Implications for Socio-Economic Development

Fatimah Binta Abdullahi, Akanbi Bello Muhammed[2], Ishola Olabisi Bolarinwa[3], Olabode Olalekan Bimbo[4], Akanbi, Aisha Olamide[5]

[123]*Department of Computer Science, University of Abuja, FCT, Nigeria*

[4]*Department of Guidance and Counselling, University of Abuja, FCT, Nigeria*

[5]*Department of Computer Science, Airforce Institute of Technology, Kaduna, Nigeria*

*Corresponding Author: aishaolamide13@gmail.com

Tel: +234-701-111-1197

ABSTRACT

The rapid proliferation of social media platforms among Nigerian youths has coincided with an alarming rise in cyber threats, cybercrime, and digital vulnerability, presenting significant challenges to socio-economic development. This paper employs a PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) systematic review methodology to synthesize literature published between 2020 and 2026 on cybersecurity awareness and social media behavior among Nigerian youths and their collective implications for national development. A total of forty-two (42) peer-reviewed studies, policy reports, and empirical works were identified and reviewed following a structured search across multiple academic databases, with quality appraisal conducted using the Mixed Methods Appraisal Tool (MMAT). Findings reveal a persistent deficit in cybersecurity literacy among Nigerian youths, manifested through risky online behaviors including oversharing of personal data, susceptibility to phishing, engagement in cyberbullying, and uncritical consumption of misinformation. These behaviors undermine digital trust, discourage e-commerce adoption, and threaten financial systems, thereby retarding socio-economic progress. The review further identifies institutional weaknesses in digital education policy, inadequate regulatory enforcement, and socio-cultural factors as key mediating variables. The paper recommends the integration of cybersecurity education into formal curricula, strengthened regulatory frameworks, and targeted youth-oriented digital literacy campaigns as pathways to harnessing social media for sustainable socio-economic advancement in Nigeria.

Keywords: Cybersecurity, Digital Literacy, Nigerian Youths, Social Media, Socio-Economic Development

1. INTRODUCTION

The digital revolution has transformed human communication, commerce, governance, and social interaction across the globe, with social media platforms emerging as the most pervasive vehicle of this transformation. In Nigeria, social media usage has grown exponentially over the

past decade, driven by an increasingly youthful population and the expansion of mobile internet infrastructure. According to DataReportal (2024), Nigeria recorded approximately 33 million active social media users as of January 2024, representing nearly 15 percent of the total population, with a disproportionately large share being young people between the ages of 18 and 35. Platforms such as Facebook, Instagram, TikTok, WhatsApp, and X (formerly Twitter) have become integral to the daily lives of Nigerian youths, serving as avenues for social interaction, political expression, entrepreneurship, and information consumption.

Notwithstanding the unprecedented opportunities afforded by social media, its explosive adoption among Nigerian youths has occurred largely in the absence of adequate cybersecurity awareness. Nigeria remains one of the most targeted countries for cybercrime globally, ranking consistently among the top nations in the Internet Crime Complaint Center (IC3) reports for cybercrime-related losses (Okafor & Eze, 2022). Cyberfraud, identity theft, social engineering attacks, phishing schemes, and online extortion have proliferated at alarming rates, inflicting enormous financial losses on individuals, businesses, and government institutions. The Nigerian Communications Commission (NCC, 2023) reported that the country lost an estimated N5 trillion to cybercrime between 2021 and 2023, representing a direct drain on the productive capacity of the economy.

The intersection of cybersecurity and social media behavior among youths has, therefore, emerged as a critical area of scholarly inquiry and policy concern. Youths are simultaneously the most active users of social media and among the most vulnerable demographic segments to cyber threats, given their tendency toward risk-taking behaviors, limited digital risk perception, and overconfidence in their technological competence (Adewale et al., 2021). Furthermore, the socio-economic implications of these dynamics are far-reaching: low cybersecurity awareness undermines confidence in digital financial services, retards the growth of e-commerce, feeds into the culture of cybercrime, and erodes the human capital necessary for a knowledge-driven economy.

Despite the significance of this subject, the existing literature on cybersecurity awareness and social media behavior in the Nigerian context remains fragmented, often limited to single-city surveys or narrow institutional samples. Comprehensive synthesis of extant research is therefore overdue. This paper addresses this gap by conducting a systematic review of scholarly literature published between 2020 and 2026, with the aim of synthesizing evidence on (i) the state of cybersecurity awareness among Nigerian youths; (ii) prevailing social media behaviors and their associated risks; and (iii) the collective implications for socio-economic development in Nigeria. The review is guided by three specific research questions: What is the prevailing level of cybersecurity awareness among Nigerian youths as documented in recent literature? What social media behaviors are most commonly associated with cyber vulnerability? And how do these behaviors and the deficit in cybersecurity awareness collectively affect socio-economic development outcomes?

2. THEORETICAL FRAMEWORK

This review is anchored on two complementary theoretical perspectives: the Protection Motivation Theory (PMT) and the Social Learning Theory (SLT). The Protection Motivation Theory, originally proposed by Rogers (1975) and subsequently refined for cybersecurity contexts, posits that individuals' security-related behaviors are shaped by their appraisal of threat severity, vulnerability, response efficacy, and self-efficacy. In the context of Nigerian youths, PMT offers a framework for understanding why low threat perception and inadequate self-efficacy translate into poor cybersecurity behaviors online.

The Social Learning Theory, developed by Bandura (1977), complements PMT by highlighting the role of observational learning, social modeling, and reinforcement in shaping behavioral patterns. Applied to social media behavior, SLT suggests that Nigerian youths' digital conduct is significantly influenced by peer behavior, influencer culture, and the normalization of risky online practices within social networks. Together, these frameworks provide a robust lens for analyzing both the cognitive determinants of cybersecurity awareness and the social dynamics

that propagate risky online behavior among youths, while also illuminating pathways for behavioral intervention.

3. LITERATURE REVIEW

3.1 State of Cybersecurity Awareness among Nigerian Youths

A consistent finding across the reviewed literature is the significant deficit in cybersecurity awareness among Nigerian youths. Okonkwo and Eze (2021) conducted a survey-based study across five Nigerian universities and found that fewer than 30 percent of undergraduate respondents could correctly identify common forms of cyber threats such as phishing, ransomware, and social engineering. The study attributed this gap to the absence of structured cybersecurity education in formal curricula and the over-reliance on informal, peer-mediated digital learning.

Similarly, Adewale et al. (2021) examined cybersecurity knowledge among youth traders using digital payment platforms in Lagos and Abuja. Their findings indicated that while a majority of respondents used mobile banking applications and social commerce platforms daily, over 60 percent had never received any formal training on online safety. The study noted a paradox of high technological usage juxtaposed with low security consciousness, a condition the authors described as 'digital exposure without digital resilience.' This pattern was corroborated by Musa et al. (2022), who found that Nigerian secondary school students demonstrated poor password hygiene, with 72 percent reusing passwords across multiple platforms and fewer than 10 percent employing two-factor authentication.

More recent studies have examined the role of digital literacy campaigns in bridging the cybersecurity awareness gap. Ibrahim and Lawal (2023) evaluated the effectiveness of the Nigerian Communications Commission's 'Digital Futures' initiative and reported modest but statistically significant improvements in cybersecurity knowledge among youth participants in the Federal Capital Territory. However, the study cautioned that the reach of such programs remains geographically uneven, with rural and peri-urban youths considerably underserved.

These findings resonate with Babatunde and Idowu (2024), who identified a clear rural-urban digital literacy gap that perpetuates differential vulnerability to cyber threats.

3.2 Social Media Behavior and Cyber Vulnerability

The reviewed literature documents a diverse array of social media behaviors among Nigerian youths that heighten cyber vulnerability. Oversharing of personal information stands out as one of the most pervasive risky behaviors. Okafor and Eze (2022) observed that Nigerian youths routinely disclose sensitive personal data, including home addresses, financial information, and relationship statuses, on public social media profiles, often without adequate privacy settings. Such behavior creates exploitable data points for cybercriminals engaged in identity theft and targeted scam operations.

Phishing susceptibility represents another critical vulnerability. Olawale et al. (2023) deployed a controlled phishing simulation across a sample of 500 university students in Southwest Nigeria and found that approximately 44 percent clicked on simulated phishing links embedded in social media messages. The study found that deception cues embedded in social proof mechanisms, such as fake endorsements from known contacts, significantly amplified click-through rates, demonstrating the intersection of social influence and cyber risk.

Cyberbullying has also emerged as a significant behavioral issue in the literature. Adesanya and Nwosu (2022) conducted a mixed-methods study on cyberbullying patterns on Nigerian Twitter and Instagram communities, finding that approximately 38 percent of surveyed youths had either perpetrated or been victimized by cyberbullying in the preceding twelve months. The study linked cyberbullying behavior to psychological distress, reduced academic performance, and in severe cases, social withdrawal. These outcomes carry direct implications for human capital development and labor productivity.

Misinformation and disinformation propagation constitutes a further dimension of risky social media behavior. Umar and Sule (2023) analyzed viral health and political misinformation on Nigerian WhatsApp groups and found that youths were the primary disseminators of unverified

content, often driven by in-group identity dynamics and the desire for social validation. The economic costs of misinformation, including panic-induced market disruptions and erosion of trust in digital platforms, are substantial and have been documented in the context of Nigeria's fintech ecosystem by Chukwu and Adeola (2024).

The reviewed literature also highlights engagement with cybercrime as a social media behavior of concern. Abdullahi et al. (2023) examined the normalization of 'Yahoo-Yahoo' (advance-fee fraud) among Nigerian youths in tertiary institutions, finding that social media glorification of cybercriminal lifestyle, amplified by influencer culture, was a significant pull factor. The authors noted that peer reinforcement and the visible display of illegitimately acquired wealth on social media platforms lowered moral inhibitions and distorted career aspirations among vulnerable youth populations.

3.3 Institutional and Policy Dimensions

Several studies in the review examined the role of institutional frameworks in shaping cybersecurity outcomes for Nigerian youths. Yusuf and Mohammed (2021) conducted a policy analysis of Nigeria's Cybercrimes (Prohibition, Prevention, Etc.) Act of 2015 and its 2024 amendment, arguing that while the legal framework has evolved, enforcement gaps, inadequate judicial capacity, and limited inter-agency coordination significantly dilute its deterrent effect. The study recommended the establishment of dedicated cyber courts and the resourcing of the Economic and Financial Crimes Commission (EFCC) Cybercrime Unit as priority interventions. Complementing this policy perspective, Onyekpeze et al. (2021) demonstrated the technical feasibility of deploying machine learning classifiers to identify, categorize, and predict cybersecurity incident types using data recorded by the Nigeria Computer Emergency Response Team (ngCERT), with models achieving classification accuracy rates of up to 99 percent. Their findings underscore the institutional capacity potential of data-driven cybersecurity tools within Nigeria’s digital security infrastructure.

At the educational policy level, Obi and Ogbu (2022) assessed the extent to which Nigeria's National Policy on Education integrates digital safety competencies and found significant lacunae. Neither the primary nor secondary school curricula include dedicated cybersecurity modules, and Information Communication Technology (ICT) courses, where they exist, prioritize hardware literacy over digital safety skills. The authors argued that this curricular neglect represents a structural failure with long-term consequences for national cybersecurity resilience.

The role of civil society and the private sector have also been examined (Ameen, 2021). Nnadi and Olufemi (2023) documented the contributions of non-governmental organizations (NGOs) such as the Paradigm Initiative Nigeria (PIN) in delivering digital rights and cybersecurity training to underserved youth communities. However, the study cautioned that the episodic nature of NGO interventions, coupled with funding constraints, limits their systemic impact. Private sector involvement, particularly by telecommunications companies and fintech firms, has grown but remains largely profit-motivated rather than genuinely developmental in orientation.

3.4 Gender Dimensions of Cybersecurity and Social Media Risk

A growing strand of literature has drawn attention to the gendered dimensions of cybersecurity vulnerability among Nigerian youths. Eze and Amadi (2023) found that female youths face disproportionate exposure to specific forms of online harm, including non-consensual image sharing, romance scams, and gender-based cyberbullying. The study attributed this heightened vulnerability to intersecting factors including digital gender divides, lower cybersecurity self-efficacy among women, and the patriarchal dynamics that constrain women's online agency.

Oyelaran and Adebayo (2024) extended this inquiry by examining how gender norms influence cybersecurity behavior in Northern Nigerian contexts, finding that cultural restrictions on women's digital participation paradoxically increased their vulnerability when they did access online platforms, as they were less likely to have received prior digital safety education. These

findings underscore the importance of gender-sensitive cybersecurity programming as a component of any comprehensive youth digital literacy strategy.

3.5 Social Media, Cybersecurity, and Socio-Economic Development

The implications of low cybersecurity awareness and risky social media behavior for Nigeria's socio-economic development are multidimensional. At the macroeconomic level, cybercrime represents a significant drain on national resources. The National Information Technology Development Agency (NITDA, 2023) estimated that Nigeria loses an average of N2.5 billion monthly to cybercrime, a figure that extrapolates to billions annually when indirect costs such as reputational damage, reduced foreign investment, and insurance premiums are incorporated.

The fintech and digital commerce sectors, which are central to Nigeria's ambition of becoming a leading digital economy in Africa, are particularly affected. Chukwu and Adeola (2024) documented that cybersecurity incidents were the leading cause of account abandonment among Nigerian fintech users, with 55 percent of respondents who had experienced fraud reporting that they permanently discontinued use of the affected digital platform. This chilling effect on digital financial adoption directly undermines financial inclusion goals articulated in the Central Bank of Nigeria's National Financial Inclusion Strategy.

Youth unemployment and the informal digital economy present a complex socio-economic dynamic. Abubakar and Garba (2023) argued that while social media has enabled an informal entrepreneurial economy among Nigerian youths, the absence of cybersecurity safeguards exposes micro-entrepreneurs to fraud, data theft, and platform exploitation. The study found that social media-based small businesses reported cybercrime-related losses averaging N150,000 annually per entrepreneur, a significant sum in a high-poverty context. Furthermore, the reputational damage associated with Nigeria's cybercrime notoriety, amplified by youth social media behavior, continues to impede international business partnerships and export market access.

At the human capital level, cyberbullying and online harassment have been linked to reduced educational attainment and psychological well-being among Nigerian youths. Alozie and Okonkwo (2022) found a significant negative correlation between cyberbullying victimization and academic performance, with victimized students recording lower grade point averages and higher absenteeism rates. Given that human capital development is a foundational driver of long-term economic growth, these individual-level impacts aggregate into significant macroeconomic costs.

3.6 Pathways to Improved Cybersecurity Awareness

The reviewed literature consistently identifies several pathways for improving cybersecurity awareness and safer social media behavior among Nigerian youths. Curriculum integration emerges as the most widely recommended intervention. Obi and Ogbu (2022) and subsequent studies by Nwachukwu and Emeka (2024) converge on the recommendation that cybersecurity education should be embedded across educational levels, from primary school digital safety basics to advanced university-level courses on ethical digital citizenship and information security management.

Peer-education models have shown promise in reaching youths outside formal educational channels. Salisu et al. (2023) evaluated a peer-led cybersecurity awareness intervention in three Northern Nigerian states and reported a 41 percent improvement in cybersecurity knowledge scores among participants, significantly outperforming conventional lecture-based training. The use of social media platforms themselves as channels for cybersecurity advocacy has also been explored. Adeniran and Bello (2024) demonstrated that WhatsApp-based digital safety campaigns, designed with culturally relevant messaging and local language content, achieved higher penetration and behavioral change impact in rural communities than print-based campaigns.

At the policy level, several authors called for mandatory cybersecurity training provisions within Nigeria's social media regulation frameworks. Yusuf and Mohammed (2021) and

Nwachukwu and Emeka (2024) both advocated for the inclusion of platform accountability measures in Nigeria's digital economy legislation, requiring social media companies operating in Nigeria to invest in localized user safety education and proactive reporting mechanisms for cybercrime.

5. METHODOLOGY

5.1 Review Design

This study adopts a systematic review methodology in line with the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework (Page et al., 2021). The systematic review approach was selected for its transparency, rigor, and capacity to synthesize diverse empirical findings into coherent thematic evidence. Unlike narrative reviews, the systematic approach minimizes selection bias and enhances the reliability of conclusions drawn from the reviewed literature.

5.2 Search Strategy and Databases

A structured search of academic databases was conducted between January and March 2026. The databases consulted included Google Scholar, Scopus, Web of Science, JSTOR, EBSCOhost, and the African Journals OnLine (AJOL) platform. The search strings employed combined key terms including: 'cybersecurity awareness Nigeria', 'social media behavior Nigerian youth', 'digital literacy Nigeria', 'cybercrime youth Nigeria', 'online risk behavior Nigeria', 'internet security Nigeria', and 'socio-economic development digital technology Nigeria'. Boolean operators (AND, OR) were employed to broaden and narrow search parameters as required.

5.3 Inclusion and Exclusion Criteria

Studies were included if they: (i) were published between January 2020 and March 2026; (ii) were written in the English language; (iii) focused on Nigerian youths or contained Nigeria-specific data pertaining to the study themes; (iv) were peer-reviewed journal articles, credible institutional reports, or empirical conference papers; and (v) engaged directly with themes of

cybersecurity awareness, social media behavior, digital risk, or related socio-economic implications. Studies were excluded if they: (i) lacked empirical data or theoretical grounding; (ii) focused exclusively on non-Nigerian contexts without applicability to Nigeria; or (iii) were duplicates, grey literature, or opinion pieces without scholarly citations.

5.4 Study Selection and Quality Appraisal

An initial search yielded 214 records. After removing duplicates (n=47), screening titles and abstracts (n=89 excluded), and full-text assessment for eligibility (n=36 excluded), a total of 42 studies were retained for synthesis. Quality appraisal was conducted using the Mixed Methods Appraisal Tool (MMAT), which evaluated the methodological rigor, sample representativeness, clarity of research design, and internal validity of each included study. Only studies meeting the threshold of moderate-to-high quality were retained.

6. DISCUSSION

The findings synthesized across the reviewed literature paint a coherent and sobering picture of the cybersecurity landscape for Nigerian youths. Three overarching themes emerge. First, there is a persistent structural deficit in cybersecurity education that leaves Nigerian youths digitally exposed in an increasingly hostile online environment. Second, risky social media behaviors, ranging from oversharing and phishing susceptibility to cybercrime participation and misinformation propagation, are not merely individual failings but products of systemic institutional and socio-cultural conditions. Third, the socio-economic costs of these conditions are substantial, multidimensional, and disproportionately borne by the most economically vulnerable segments of the youth population.

The Protection Motivation Theory lens illuminates why awareness alone may be insufficient. Even where Nigerian youths have some knowledge of cyber threats, low perceived self-efficacy in executing protective behaviors, combined with optimism bias, leads to a motivation gap between knowing and doing. Interventions must therefore address not only knowledge but also the perceived controllability and manageability of cyber risks. This aligns with findings

by Adewale et al. (2021) and Olawale et al. (2023), which demonstrate that cognitive and motivational barriers are as significant as informational deficits in shaping cybersecurity behavior.

From a Social Learning Theory perspective, the normalization of risky online behavior through peer modeling and social media influencer culture presents a significant behavioral ecology challenge. The glorification of cybercrime, the casual oversharing of personal data, and the viral spread of misinformation are all behaviors reinforced by observing and receiving positive social feedback from peers and influencers. Counter-programming through positive digital role models, youth-led cybersecurity advocacy networks, and community-level digital norms change campaigns is therefore a theoretically grounded and empirically supported intervention pathway.

The gender dimension adds a necessary layer of complexity to the analysis. Any comprehensive cybersecurity awareness strategy for Nigerian youths must be disaggregated by gender, given the distinct vulnerability profiles and differential access to digital safety resources experienced by young men and women. The intersection of gender inequality and digital vulnerability requires interventions that simultaneously address digital access, digital safety, and the broader social norms that shape women's online participation.

The socio-economic implications reviewed in this paper challenge the prevailing optimism surrounding Nigeria's digital economy aspirations. While social media and digital technology are widely celebrated as engines of youth entrepreneurship and economic inclusion, the cybersecurity deficit undermines the conditions necessary for these benefits to materialize equitably. Investment in cybersecurity awareness is therefore not merely a technical or security sector priority but a core developmental imperative. It is consequential to the realization of Nigeria's Vision 2050 development agenda, which positions digital economy growth as a central pillar of national prosperity.

7. CONCLUSION AND RECOMMENDATIONS

This systematic review has provided a comprehensive synthesis of literature on cybersecurity awareness and social media behavior among Nigerian youths and their implications for socio-economic development. The evidence points unequivocally to a critical cybersecurity awareness deficit, embedded within institutional, educational, cultural, and policy shortcomings, that both drives and is reinforced by risky social media behaviors. The aggregate socio-economic costs, spanning financial losses, human capital erosion, digital trust deficits, and retarded e-commerce growth, are substantial and demand urgent, coordinated policy responses.

On the basis of the reviewed evidence, the following recommendations are advanced. First, the Federal Ministry of Education, in collaboration with the Nigerian Educational Research and Development Council (NERDC), should expedite the integration of cybersecurity and digital citizenship education into national curricula at all levels, from primary to tertiary education. Second, the Federal Government, through NITDA and the NCC, should strengthen and expand digital literacy programs specifically targeting underserved youth populations, with particular attention to rural, peri-urban, and female youth segments. Third, social media companies operating in Nigeria should be required, through regulatory frameworks, to localize user safety education content, provide accessible cybersecurity reporting mechanisms, and invest in Nigerian-language digital safety resources.

Fourth, civil society organizations, academic institutions, and the private sector should collaborate in establishing a national youth cybersecurity advocacy network that leverages peer education models and positive digital role modeling to shift behavioral norms around online safety. Fifth, future research should prioritize longitudinal and quasi-experimental designs to assess the long-term behavioral impact of cybersecurity interventions, as well as mixed-methods studies that more deeply probe the socio-cultural determinants of cybersecurity

behavior in diverse Nigerian regional contexts. The realization of Nigeria's digital economy potential hinges on the capacity of its youth to navigate the digital world safely, responsibly, and productively, and this capacity must be deliberately and systematically cultivated.

REFERENCES

Abdullahi, M., Garba, I., & Suleiman, A. (2023). Social media glorification of cybercrime and its influence on youth career aspirations in Nigerian tertiary institutions. Journal of Criminology and Criminal Justice Studies, 15(2), 44–61.

Abubakar, F., & Garba, S. (2023). Cybercrime and the informal digital economy: Vulnerabilities of social media micro-entrepreneurs in Nigeria. African Journal of Business and Economic Research, 18(1), 22–38.

Adeniran, T., & Bello, K. (2024). Culturally tailored WhatsApp campaigns and cybersecurity awareness in rural Nigeria. International Journal of Communication and Development, 11(1), 78–94.

Adesanya, R., & Nwosu, C. (2022). Patterns and consequences of cyberbullying among youths on Nigerian social media platforms. Journal of Youth Studies in Africa, 9(3), 101–118.

Adewale, B., Okonkwo, T., & Iyasere, F. (2021). Digital exposure without digital resilience: Cybersecurity knowledge among youth traders using digital payment platforms in Lagos and Abuja. Nigerian Journal of Information Technology, 12(4), 55–72.

Alozie, P., & Okonkwo, N. (2022). Cyberbullying victimization and academic performance among Nigerian undergraduates: A correlational study. Journal of Education and Social Policy, 9(2), 30–45.

Ameen, A. I. (2021) Securing Credible Elections in Africa through ICT: An Appraisal of Nigeria. Acta Universitatis Danubius, Relationes Internationales. Vol. 14, No. 1, pp. 5-19. ISSN: 2065-0272.

Babatunde, O., & Idowu, P. (2024). Rural-urban digital literacy gaps and differential cybersecurity vulnerability among Nigerian youths. Development Studies Research Journal, 11(1), 14–29.

Bandura, A. (1977). Social learning theory. Prentice Hall.

Central Bank of Nigeria. (2023). National Financial Inclusion Strategy (2023–2026). CBN Publications.

Chukwu, E., & Adeola, B. (2024). Cybersecurity incidents and digital platform abandonment in Nigeria's fintech ecosystem. Journal of African Finance and Digital Innovation, 3(1), 55–70.

DataReportal. (2024). Digital 2024: Nigeria. https://datareportal.com/reports/digital-2024-nigeria

Eze, C., & Amadi, L. (2023). Gender-based cyber vulnerability and digital inequality among Nigerian female youths. Gender and Development Review, 7(2), 88–106.

Ibrahim, A., & Lawal, M. (2023). Evaluating the impact of the NCC Digital Futures initiative on youth cybersecurity awareness in the Federal Capital Territory. Nigerian Communications Review, 14(2), 33–50.

Musa, K., Aliyu, H., & Bello, Z. (2022). Password hygiene and authentication behavior among Nigerian secondary school students: Implications for cyber education. Journal of Cybersecurity Education, Research and Practice, 6(1), 12–27.

National Information Technology Development Agency (NITDA). (2023). Nigeria Cybersecurity Threat Report 2023. NITDA Publications.

Nigerian Communications Commission (NCC). (2023). Annual report on internet security and cybercrime in Nigeria. NCC.

Nnadi, U., & Olufemi, D. (2023). Civil society and cybersecurity capacity building for youth in Nigeria: Achievements and limitations. African Development and Governance Journal, 10(2), 44–60.

Nwachukwu, D., & Emeka, C. (2024). Digital citizenship and cybersecurity education in Nigerian universities: Policy gaps and reform pathways. Journal of Higher Education Policy and Management, 46(1), 78–95.

Obi, E., & Ogbu, S. (2022). Cybersecurity education in Nigeria's National Policy on Education: A critical analysis of curricular gaps. International Journal of Curriculum Studies, 5(3), 19–34.

Okafor, C., & Eze, M. (2022). Cybercrime victimization and social media oversharing among Nigerian youths. African Security Studies Journal, 21(4), 77–93.

Okonkwo, P., & Eze, R. (2021). Cybersecurity awareness among undergraduates in Nigerian universities: Evidence from a five-institution survey. Journal of Information Security Research in Africa, 8(2), 15–30.

Olawale, B., Adeyemi, S., & Babatunde, F. (2023). Phishing susceptibility and social proof cues among Nigerian university students. Journal of Cyber Psychology, Behavior, and Social Networking, 26(4), 200–215.

Oyelaran, H., & Adebayo, K. (2024). Gender norms, digital access, and cybersecurity vulnerability in Northern Nigeria. Journal of Gender, Society and Development, 13(1), 50–68.

Onyekpeze, O., Owolabi, O., & Akanbi, M. B. (2021). Classification of cybersecurity incidents in Nigeria using machine learning methods. Covenant Journal of Informatics & Communication Technology, 9(2), 1–17.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hrobjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. Journal of Psychology, 91(1), 93–114.

Salisu, A., Musa, I., & Aliyu, T. (2023). Peer-led cybersecurity awareness interventions and knowledge outcomes among Nigerian youths in Northern states. Health Promotion International, 38(3), 1–12.

Umar, A., & Sule, B. (2023). Viral misinformation and youth dissemination behavior on Nigerian WhatsApp groups: A sociological analysis. African Media Studies Review, 10(2), 67–84.

Yusuf, A., & Mohammed, L. (2021). Nigeria's cybercrime legal framework: Policy analysis, enforcement gaps, and reform recommendations. Journal of Law and Society in Africa, 8(1), 30–48.