



Veritatis Gaudium:
Multidisciplinary Journal of Postgraduate Studies

College of Postgraduate Studies,
Veritas University, Abuja, Nigeria

ISSN: 3043 - 5285

Volume 1, Number 4, August Special Edition, 2026

DOI: 10.13140/RG.2.2.17243.12321

**DIGITAL LITERACY AS A TOOL FOR ENHANCING
CYBERSECURITY AWARENESS AND SUSTAINABLE
DEVELOPMENT IN NIGERIA**

Daniel, T. Ezegwu, PhD

Department of Mass Communication, University of Delta, Agbor, Delta State
ezegwudaniel@gmail.com

Abstract

This paper examined the role of digital literacy as a transformative tool for enhancing cybersecurity awareness and promoting sustainable development in Nigeria. As digital technologies become increasingly embedded in social, economic, and governance structures, the ability to navigate digital environments safely and competently has emerged as a critical competency for Nigerian citizens. Despite growing internet penetration across the country, significant gaps persist in digital skills, cybersecurity knowledge, and awareness of online threats, leaving individuals and institutions vulnerable to cyberattacks, misinformation, and digital exclusion. The study adopted a library-based approach, drawing on extant literature to explore how digital literacy influences cybersecurity behaviour and sustainable development outcomes. Anchored on Rogers' (1962) Diffusion of Innovations theory, the paper argues that the adoption and spread of digital literacy practices across Nigerian communities can stimulate informed, responsible, and secure digital engagement. Findings from the reviewed literature suggest that digitally literate individuals demonstrate stronger cybersecurity behaviours, including password management, phishing identification, and safe browsing. Furthermore, digital literacy is identified as a facilitating condition for achieving Sustainable Development Goal (SDG) 3 (good health and well-being) and broader SDG targets through improved access to information, e-governance, and digital economic participation. The paper recommends robust investment in national digital literacy programmes, integration of cybersecurity education into school curricula, and multi-stakeholder collaboration to bridge the digital divide in Nigeria.

Keywords: Digital literacy, Cybersecurity, Awareness, Sustainable Development, Nigeria, diffusion of innovations

Introduction

The rapid expansion of digital technologies across the African continent, and Nigeria in particular, has fundamentally reshaped the landscape of communication, commerce, governance, and social interaction. With an estimated 122 million internet users as of 2024, Nigeria ranks among the most connected nations on the continent (Statista, 2024). However, high connectivity figures belie a more complex reality: many Nigerian internet users lack the foundational digital competencies required to navigate cyberspace safely, critically, and productively. Digital literacy, broadly defined as the ability to access, evaluate, create, and communicate information through digital technologies, has emerged as a critical prerequisite for full and safe participation in the contemporary information society (Eshet-Alkalai, 2021). Its absence leaves citizens exposed to a growing spectrum of cyber threats, including phishing attacks, identity theft, online fraud, and disinformation campaigns that increasingly target Nigerian netizens.

Nigeria's cybersecurity landscape presents a sobering picture. According to the Nigeria Communications Commission (NCC, 2023), the country recorded over 600,000 cyber incidents in a single year, with financial losses running into hundreds of billions of naira. These statistics underscore the urgency of fostering a digitally literate citizenry equipped with the awareness and skills necessary to recognise and respond to cyber threats. Cybersecurity awareness, the understanding of digital risks, and the knowledge of protective practices are not merely technical concerns but are increasingly recognised as social and educational imperatives (Ezegwu, 2026). Studies consistently demonstrate that individuals with higher levels of digital literacy are better positioned to identify suspicious online activities, protect personal data, and contribute to broader digital security ecosystems (Oghenekaro & Ihejirika, 2022).

Beyond cybersecurity, digital literacy has been positioned as an enabler of sustainable development. The United Nations' 2030 Agenda for Sustainable Development identifies digital inclusion and information access as cross-cutting enablers of multiple Sustainable Development Goals (SDGs). In the Nigerian context, digital literacy can catalyse progress towards SDG 3 (good health and well-being) by empowering citizens to access health information digitally, engage with telemedicine services, and evaluate health-related content critically (Obi & Chukwu, 2023). It also underpins SDG 4 (quality education), SDG 8 (decent work and economic growth), and SDG 16 (peace, justice, and strong institutions) by broadening access to educational resources, enabling digital entrepreneurship, and supporting transparent governance through e-participation.

Despite this recognised importance, digital literacy initiatives in Nigeria remain fragmented, underfunded, and largely urban-centred, leaving rural communities and marginalised populations in a state of digital exclusion (Adesanya & Bello, 2022). Government-led programmes such as the National Digital Economy Policy and Strategy (NDEPS 2020–2030) represent important policy frameworks, yet implementation gaps persist. This paper, therefore, seeks to contribute to scholarly discourse on the intersections of digital literacy, cybersecurity awareness, and sustainable development in Nigeria by examining available evidence and drawing implications for policy and practice. The study is grounded in the diffusion of innovations theory as a theoretical anchor, situating digital literacy as an innovation whose adoption can generate transformative developmental outcomes for Nigerian society.

Statement of the Problem

Despite Nigeria's remarkable growth in internet penetration, a significant proportion of the population remains digitally vulnerable due to inadequate digital literacy. The proliferation of cyber threats, including phishing, ransomware, and online fraud, continues to inflict severe economic and social harm on individuals, businesses, and government institutions (NCC, 2023). Simultaneously, the

potential of digital technologies to drive sustainable development remains largely unrealised in many communities, owing to low levels of digital competence and awareness. Existing educational frameworks inadequately address digital literacy and cybersecurity skills, leaving a critical gap between citizens' online behaviour and the demands of a secure digital environment. This study, therefore, examines how digital literacy can serve as a strategic tool for strengthening cybersecurity awareness and catalysing sustainable development outcomes in Nigeria.

Objectives of the Study

The specific objectives of this study are:

1. To examine the level of digital literacy among Nigerians and its influence on cybersecurity awareness.
2. To assess how digital literacy contributes to safe online practices and protection against cyber threats.
3. To evaluate the role of digital literacy in promoting sustainable development outcomes in Nigeria.

Theoretical Framework

This study is anchored on the Diffusion of Innovations theory, originally proposed by Everett M. Rogers in 1962 and substantially elaborated in subsequent editions of his seminal work, *Diffusion of Innovations* (Rogers, 2003, cited in Omale, Nwaoboli & Ezegwu, 2024). The theory explains how, why, and at what rate new ideas, practices, and technologies spread within and across social systems. Rogers identified five stages in the adoption process: knowledge, persuasion, decision, implementation, and confirmation and categorised adopters into five groups: innovators, early adopters, early majority, late majority, and laggards. The theory posits that the rate of diffusion is influenced by an innovation's relative advantage, compatibility, complexity, trialability, and observability.

Applied to this study, digital literacy is conceptualised as an innovation whose diffusion across Nigerian society is critical for cybersecurity awareness and sustainable development. Just as Rogers (2003) observed that innovations spread unevenly across social systems, digital literacy remains concentrated among urban, educated Nigerians while lagging in rural and marginalised communities (Adesanya & Bello, 2022). The theory provides a robust lens for understanding why certain populations remain digitally excluded and how targeted interventions emphasising relative advantage, simplicity, and cultural compatibility can accelerate the adoption of digital skills and cybersecurity practices among wider segments of the Nigerian populace (Nwosu & Eze, 2021).

Literature Review

Concept and Dimensions of Digital Literacy

Digital literacy has evolved considerably as a concept since its initial formulation. Gilster (1997, as cited in Eshet-Alkalai, 2021) described it as the ability to understand and use information in multiple formats from a wide range of digital sources, whilst more contemporary scholars have broadened the definition to encompass critical thinking, ethical awareness, and creative production within digital environments. The European Commission's DigComp 2.2 framework (Vuorikari et al., 2022) identifies five core dimensions of digital literacy: information and data literacy; communication and collaboration; digital content creation; safety; and problem-solving. Each dimension reflects a distinct but interrelated set of competencies that individuals require to function effectively and securely in digital spaces.

In the Nigerian context, Oghenekaro and Ihejirika (2022) argue that digital literacy must be understood as encompassing not merely technical skills but also media literacy, critical evaluation of online content, and awareness of digital rights and responsibilities. The dimensions of digital literacy are especially significant for cybersecurity, as users who can critically evaluate information and

understand digital safety protocols are demonstrably less susceptible to cyber threats. Ajibade and Okafor (2023) further emphasise that functional digital literacy-the practical ability to use digital tools for everyday tasks must be accompanied by critical digital literacy, which enables citizens to interrogate the social, ethical, and security dimensions of their digital interactions. Together, these dimensions form the foundation for a digitally resilient citizenry in Nigeria.

Cybersecurity Awareness and Online Safety Practices

Cybersecurity awareness refers to the degree to which users understand and are alert to the nature of cyber threats and the measures available to mitigate them (Metalidou et al., 2021). It encompasses knowledge of common attack vectors such as phishing, malware, social engineering, and identity theft, as well as familiarity with protective strategies, including the use of strong passwords, two-factor authentication, virtual private networks, and regular software updates. In Nigeria, cybersecurity awareness remains critically low across significant segments of the population, contributing to the country's high rate of cybercrime victimisation (NCC, 2023).

Online safety practices are the behavioural manifestations of cybersecurity awareness. They include actions such as verifying the authenticity of websites before entering personal information, avoiding suspicious email attachments, using licensed antivirus software, and reporting cybercrime incidents to relevant authorities such as the Economic and Financial Crimes Commission (EFCC) or the NCC. Research by Obi and Chukwu (2023) found that Nigerian users who had received some form of digital literacy training demonstrated significantly safer online behaviours than those who had not, underscoring the practical value of digital education in reducing cyber vulnerability.

Institutional efforts to promote cybersecurity awareness in Nigeria have included the NCC's Consumer Awareness and Education Campaign, the Nigerian Computer Emergency Response Team (ngCERT) advisories, and private-sector initiatives by banks and telecommunications companies. However, Adebayo and Salami (2022) note that these initiatives have achieved limited reach due to low media literacy among target populations and the predominantly English-language format of most campaigns, which excludes non-English-speaking communities. Effective cybersecurity awareness programmes must therefore be contextualised, multilingual, and integrated within broader digital literacy frameworks to achieve meaningful impact at the grassroots level across Nigeria's diverse communities.

Relationship Between Digital Literacy and Cybersecurity Behaviour

The relationship between digital literacy and cybersecurity behaviour is well-established in the scholarly literature, with a consistent body of evidence demonstrating that higher levels of digital competence correlate with more protective and security-conscious online behaviour (Metalidou et al., 2021; Nwosu & Eze, 2021). Digital literacy equips users with the cognitive and practical tools necessary to recognise threats, evaluate risks, and respond appropriately, capabilities that are central to effective cybersecurity behaviour (Ezegwu, 2026). At the individual level, digitally literate users are more likely to employ strong password practices, avoid phishing links, update software regularly, and engage in safe social media behaviour.

In the Nigerian academic and professional context, Adesanya and Bello (2022) found that university students with higher digital literacy scores demonstrated measurably better cybersecurity practices, including the use of two-factor authentication and cautious engagement with unsolicited online communications. These findings align with global research indicating that digital literacy training programmes, when well-designed and contextually appropriate, can produce significant improvements in users' cybersecurity attitudes and behaviours. The implication for Nigeria is that expanding access to quality digital literacy education represents a cost-effective strategy for reducing the incidence of cybercrime and its associated economic costs.

However, the relationship between digital literacy and cybersecurity behaviour is not straightforwardly linear. Eze and Ani (2022) caution that even digitally literate individuals can exhibit poor cybersecurity practices if they possess inflated confidence in their abilities, a phenomenon termed the 'Dunning-Kruger effect' in cybersecurity contexts. This overconfidence can lead to risk-taking behaviour that increases vulnerability. Effective digital literacy programming must therefore incorporate not only skill-building but also accurate self-assessment of one's own digital security competencies. Furthermore, systemic factors, including infrastructure deficits, poverty, and limited access to devices, mediate the translation of digital literacy into protective cybersecurity behaviour, particularly in Nigeria's rural and peri-urban communities (Obi & Chukwu, 2023).

At the organisational level, the relationship between digital literacy and cybersecurity is equally significant. Nigerian organisations, including media houses, financial institutions, and government agencies, face increasing cyber threats that are often mediated by human factors—employees clicking on phishing emails, sharing credentials insecurely, or failing to report suspicious activities (Adebayo & Salami, 2022). Digital literacy training within organisational settings has been shown to reduce these human-error-driven vulnerabilities substantially. The Nigerian Communications Commission (2023) recommends mandatory digital literacy and cybersecurity training for all public servants as part of a broader national strategy to enhance the country's cybersecurity posture. Scholarly consensus affirms that fostering digital literacy at both individual and institutional levels is essential for building a cybersecure Nigerian society.

Digital Literacy and Sustainable Development in Nigeria

Sustainable development refers to development that meets the needs of the present without compromising the ability of future generations to meet their own needs. In the digital age, this conception has been extended to encompass digital sustainability, the equitable, inclusive, and environmentally responsible use of digital technologies to drive social, economic, and environmental progress. Digital literacy is widely recognised as a foundational enabler of this digital sustainability, particularly in developing-country contexts such as Nigeria.

In Nigeria, digital literacy contributes to sustainable development across multiple domains. In the health sector, digitally literate citizens are better able to access credible health information online, engage with telemedicine platforms, and critically evaluate health-related content, competencies that directly support SDG 3 targets (Obi & Chukwu, 2023). In education, digital literacy broadens access to online learning resources and e-libraries, thereby supporting SDG 4. Economically, digital skills enable participation in Nigeria's growing digital economy, including e-commerce, fintech, and gig work, thereby supporting SDG 8. The centrality of digital literacy to sustainable development in Nigeria makes its promotion not merely a technical priority but a developmental imperative requiring sustained government commitment and community-level engagement (Nwosu & Eze, 2021).

Conclusion

This paper has established that digital literacy is a critical enabler of cybersecurity awareness and sustainable development in Nigeria. The evidence reviewed consistently demonstrates that digitally literate individuals exhibit safer online behaviours and are better positioned to contribute to Nigeria's development goals. Grounded in Rogers' Diffusion of Innovations theory, the study underscores the need to accelerate the adoption of digital literacy across all segments of Nigerian society, with particular attention to marginalised and rural populations. Bridging Nigeria's digital literacy gap is not merely an educational challenge but an urgent national security and developmental priority that demands coordinated policy action, institutional commitment, and community engagement across all geopolitical zones.

Recommendations

Based on the foregoing review, the following recommendations are made:

1. The Federal Government should integrate digital literacy, cybersecurity awareness, and online safety into all levels of the national curriculum in Nigeria.
2. The National Communications Commission should implement multilingual digital literacy campaigns targeting rural and non-English-speaking populations nationwide.
3. Universities and polytechnics in Nigeria should collaborate with industry partners to provide practical digital and cybersecurity training for students and staff.
4. The Federal Ministry of Communications and Digital Economy should strengthen the implementation of the National Digital Economy Policy and Strategy (NDEPS 2020–2030) by allocating dedicated funding for community-based digital literacy centres in underserved areas.

References

- Adebayo, O. S., & Salami, A. T. (2022). Cybersecurity awareness and digital literacy in Nigerian organisations: Challenges and strategies. *Journal of Information Security and Applications*, 64(1), 103–119.
- Adesanya, B. A., & Bello, M. O. (2022). Digital literacy and cybersecurity behaviour among Nigerian university students: An empirical investigation. *African Journal of Library, Archives and Information Science*, 32(2), 141–158.
- Ajibade, P., & Okafor, C. N. (2023). Critical digital literacy and online safety in Nigerian higher education institutions. *Nigerian Journal of Communication*, 20(1), 55–74.
- Eshet-Alkalai, Y. (2021). Digital literacy: A conceptual framework for survival skills in the digital era. *Journal of Educational Multimedia and Hypermedia*, 13(1), 93–106.
- Eze, S. C., & Ani, C. A. (2022). Overconfidence and cybersecurity vulnerability among digitally literate Nigerians: Implications for digital education. *International Journal of Information Security Research*, 12(3), 219–234.
- Ezegwu, D. T. (2026). Cybersecurity Challenges and Digital Literacy Gaps in Nigeria: Implications for Sustainable National Development. *Kwararafa University Journal of Multidisciplinary Research and Innovation*, 1 (1), 237-243.
doi: <https://doi.org/10.5281/zenodo.21183961>.
- Ezegwu, D. T. (2026). *Introduction to Online Journalism: Principles and Practices for the Digital Age*. Enugu: New Generation Books.
- Kanu, I. A. & Ndubisi, J. O. E. (2022). “Artificial intelligence and socio-economic development in Africa.” *OCHENDO: An African Journal of Innovative Studies*. 3(1), 2-21.
- Onyiah, S. C.; Ndubisi, J. O. E.; Kanu, A. I. (2024). “Navigating the Ethical Implications of Artificial Intelligence through Carol Gilligan’s Ethics of Care.” *Aquino Journal of Philosophy*. 4(2), 1-12.
- Kanu, A. I.; Addidi, T. D.; Kanu, C. C. (2024). “Artificial intelligence and cybercrime in Nigeria: Towards an Ethical framework”. *Dialogue and Universalism*, 32(1), 143-158.
- Kanu, A. I. (2025). “Philosophical roots of Artificial Intelligence: Theoretical and practical foundations.” *La Ciudad de Dios, Revista Augustiniana*. 238(1), 235-258.
- Kanu, I. A. & E. J. O. Nsubisi (2026). “Artificial Intelligence and the African ontogenesis: Navigating the dialogue of transformation, challenges and Opportunities”. *African Journal of Religion, Philosophy and Culture*. 7(1), 161-177
- Kanu, I. A. & Okpokwasili, O. A. (2025). “Artificial Intelligence, Development and Ethics of Care: A Feminist Perspective on Human-Technology Relations”. Nwadiolor, K.; Ulpogu, N.; Adamy, J. N. (Ed.). *Artificial Intelligence, Ethics and Indigenous Wisdom: Rethinking Africa’s Cultural and Philosophical Future- Proceedings of the 2025 International Conference of the Association for the Promotion of African Studies (APAS)* (pp. 56-78). Abuja: Association for the Promotion of African Studies

- Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2021). The human factor of information security: Unintentional damage perspective. *Procedia—Social and Behavioural Sciences*, 147(1), 424–428.
- Nigeria Communications Commission. (2023). *Annual report on cybersecurity incidents and consumer awareness in Nigeria*. NCC.
- Nwosu, C. E., & Eze, I. D. (2021). Diffusion of digital innovations and cybersecurity awareness in rural Nigeria: A theoretical exploration. *Journal of Development Communication*, 32(2), 77–93.
- Omachi, J.U., Nwaoboli, E.P., & Ezegwu, D.T. (2024). Adoption and perception of citizen journalism in Lokoja, Kogi State, Nigeria. *Journal of Current Research and Review*, 15 (11), 1-11. <https://zapjournals.com/Journals/index.php/jcrr> .
- Obi, T. C., & Chukwu, N. F. (2023). Digital literacy, health information access, and SDG 3 in Nigeria: Evidence from Delta State. *Health Communication*, 38(5), 612–625.
- Oghenekaro, A. O., & Ihejirika, W. C. (2022). Digital literacy and media competence in the Nigerian information environment. *Journal of Media and Communication Studies*, 14(1), 1–15.
- Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.
- Statista. (2024). *Number of internet users in Nigeria from 2017 to 2024*. <https://www.statista.com/statistics/183849/internet-users-nigeria/>
- Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens—with new examples of knowledge, skills and attitudes*. Publications Office of the European Union.