Journal of Adult Education in Tanzania (JAET)
June, 2026, Vol. 28, Issue 1 pp. 79-98
eISSN 29616271 / pISSN 27389243

DOI: https://doi.org/*10.61408/jaet2026v28i01.04*

The Role of Lifelong Digital Literacy in Preventing Online Victimisation in Nigeria

Isma'il Husain Mshelia

University of Abuja, Abuja Nigeria

Email: mshelia.ismail@uniabuja.edu.ng

ORCID ID: http://orcid.org/0000-0002-7642-709X

Received: 30/01/2026 *Revised: 03/05/2026* *Accepted: 16/06/2026* *Published: 30/06/2026*

Abstract

The digital transformation of modern life has brought unprecedented risks in the form of cybercrimes, a phenomenon that disproportionately affects individuals with limited digital skills. Globally, millions of Internet users have experienced some form of online victimisation, including phishing, identity theft, cyberbullying, and online fraud. This study explores the role of lifelong digital literacy as a potential protective mechanism for reducing vulnerability to online victimisation, focusing on vulnerable populations such as older adults, low-income groups, and residents of digitally underserved regions, particularly in Nigeria. Drawing on Routine Activity and social learning theoretical perspectives, the study conceptualises digital literacy as not only a technical skill but also an evolving form of capable guardianship and behavioural adaptation alongside secure systems, regulation, reporting mechanisms, and organisational responsibility. This study adopted a desk-based narrative review methodology with thematic synthesis to critically examine secondary literature from peer-reviewed journal articles, academic books, policy documents, and other sources. Through a thematic synthesis of the reviewed literature, this study identifies critical shortcomings in current digital literacy initiatives, including limited reach, inadequate contextualisation, and poor integration into crime prevention frameworks. The findings further suggest that integrating culturally relevant digital education into local communities may reduce vulnerability, enhance digital resilience, and improve online safety outcomes for

high-risk groups in the future. While some evidence from Nigeria supports these observations, broader conclusions are informed by international studies with potential relevance to the Nigerian context. Therefore, this study recommends implementing lifelong, inclusive, and context-sensitive digital education strategies embedded in public policy and tailored to the lived realities of at-risk populations to help reduce vulnerability to cyber victimisation across the life course.

Keywords: Cybercrime, digital literacy, victimization, lifelong learning.

How to cite: Mshelia, I. H. (2026). The role of lifelong digital literacy in preventing online victimisation in Nigeria. *Journal of Adult Education in Tanzania*, *28*(1), 79–98. https://doi.org/*10.61408/jaet2026v28i01.04*

Introduction

The digital age has revolutionised human interaction, commerce, education, and communication. However, the same technological advancements that offer convenience and connectivity have also introduced new avenues for victimisation through cybercrimes. Online fraud, identity theft, phishing, ransomware, and cyberbullying, among other things, affect a significant percentage of internet users globally. The scale and complexity of these threats are intensifying, particularly as more people, regardless of age or socioeconomic status, rely on digital platforms in their daily lives (Abdullah et al., 2025). Despite increasing awareness of cybersecurity issues, a significant digital divide persists in terms of users' ability to understand and manage risks leading to online victimisation 'harmful actions directed at an individual or group via the internet, including threats, harassment, stalking, sexual solicitation, and exploitation, often involving psychological or emotional harm' (Mitchell et al., 2011). Many individuals, especially older adults, low-income populations, and those with limited formal education, lack the digital literacy skills required to recognise and respond to threats effectively. These populations are more likely to fall victim to scams, misinformation, and other forms of cyber exploitation (Ani & Batisai, 2024).

While government and private initiatives are attempting to address online safety through campaigns and school-based education, most of such efforts focus predominantly on youth or technology professionals. There remains a critical gap, particularly across many low and middle-income countries, in promoting digital literacy 'the ability to use information and communication technologies to find, evaluate, create, and communicate information, requiring both cognitive and

technical skills' (American Library Association, 2011) that spans across all age groups and socio-economic categories especially in the global south. Lifelong learning is increasingly recognised as a vital strategy to ensure digital inclusion and resilience. It is conceptualized by UNESCO Institute for Lifelong Learning (UIL, 2022) as a life-wide process that combines learning and living, involving people of all ages in diverse learning activities, contexts, and modalities aimed at satisfying a broad range of learning needs and aspirations. Building on this principle, lifelong digital literacy is referred to as the continuous acquisition, refinement, and application of digital knowledge, skills, and critical competencies throughout the life course in response to evolving technologies and online environments (Ng, 2012; Vuorikari et al., 2022). This requires continuous updating as digital platforms, information ecosystems, and cyber threats evolve. Consequently, lifelong digital literacy contributes to digital inclusion, informed online participation, and the development of competencies that may reduce individuals' vulnerability to online victimisation.

Against this backdrop, this study explores the intersection between education and cybercrime prevention. This study explicates how continuous learning can serve as a protective factor against cybercrime, particularly for vulnerable populations such as older adults, low-income groups, rural dwellers, individuals with limited access to formal education, and residents of digitally underserved regions, particularly Nigeria. Thus, this study contributes to the knowledge and efforts to integrate digital literacy into national crime prevention agendas.

The literature on cybercrime has grown extensively over the last two decades because of the increasing digitisation of socioeconomic life. One of the most influential early classifications was proposed by Wall (2007), who categorised cybercrimes into four types: cyber-trespass, cyber-deception/theft, cyber pornography/obscenity, and cyber violence. While this classification remains influential in cybercrime scholarship, more recent frameworks have provided broader and more nuanced understandings of contemporary cybercrime. For example, a taxonomy developed by the National Academies of Sciences, Engineering, and Medicine (NASEMS, 2025) classifies cybercrime into the following six broad categories: acts targeted against machines, data, or systems; fraud and acts targeted against property; acts against individuals (nonsexual); acts against individuals (sexual); acts targeted against groups; and acts involving incidental technology use. The framework further distinguishes offences according

to the degree of cyber involvement, ranging from cyber-dependent to cyber-assisted crimes (see Appendix 1). This broader classification captures emerging threats, such as ransomware, cyberstalking, online fraud, and technology-facilitated violence, thereby providing a more comprehensive understanding of the contemporary cybercrime landscape. Among these various forms of cybercrime, cyber deception and fraud including phishing, online scams, and identity theft remain particularly relevant to discussions of digital literacy because they exploit users' limited ability to identify and respond to online risks. Studies have consistently shown that digital literacy and digital inclusion are associated with an individual's capacity to recognise, assess, and manage such threats effectively (Livingstone & Helsper, 2007; van Deursen & van Dijk, 2014; Vuorikari et al., 2022).

While adult users face high levels of online victimisation, most studies on digital literacy focus on children and adolescents. This narrow focus creates a significant gap in understanding the risks faced by vulnerable adult populations, such as older adults and individuals in marginalised communities, who may not benefit from school-based or workplace digital education initiatives. Furthermore, digital literacy is often treated as a fixed or technical skill set rather than a dynamic and evolving process of knowledge acquisition that must continue throughout life. This static conceptualisation limits the development of holistic interventions that recognise learning as an ongoing need in the face of rapidly changing digital threats. Although UIL (2020) underscored the relevance of lifelong learning in preparing individuals to adapt to evolving societal challenges, this principle remains under-explored in the digital safety literature.

Another gap lies in the minimal integration of criminological theories into digital literacy and cybercrime prevention strategies. For example, Cohen and Felson's (1979) Routine Activity Theory (RAT) and Bandura's (1977) Social Learning Theory (SLT) offer valuable insights into how continuous digital education can function as a form of prevention. According to RAT, crime is more likely to occur when there is a motivated offender, a suitable target, and the absence of a capable guardian. In the context of cybercrime, digital literacy has the potential to function as a component of capable guardianship alongside secure systems, regulations, reporting mechanisms, and organisational responsibility. Thus, it can reduce vulnerability and equip individuals to protect themselves from becoming targets. Similarly, SLT emphasises that individuals learn behaviours through observation

and reinforcement. Through sustained digital education, individuals can learn positive online behaviours and develop resistance to fraudulent or harmful digital content. However, despite the theoretical value of these frameworks, few studies have explicitly applied them to lifelong digital literacy.

In addition, there is a notable gap in qualitative desk reviews that focus on vulnerable adult populations and integrate criminological theories to assess how digital literacy can evolve into a lifelong protective mechanism against online victimisation. This theoretical underutilisation limits a comprehensive understanding of the behavioural and structural benefits of ongoing digital education. As most evaluations of digital literacy programmes emphasise short-term outcomes or institutional training effectiveness, there is a need for more desk-based syntheses that consolidate insights from diverse sources to explore the long-term societal implications of digital literacy for crime prevention. In addition, the available empirical literature on lifelong digital literacy and online victimisation within the Nigerian context is relatively limited. This study seeks to address these limitations by conducting a structured synthesis of the secondary literature to critically analyse the protective potential of lifelong digital literacy. Although the study focuses on Nigeria, it synthesises both Nigerian and international literature to identify evidence that is directly relevant to the Nigerian context.

Methodology

This study adopted a qualitative research design based on a narrative desk review methodology. The goal was to synthesise and critically examine secondary literature from diverse sources to understand the role of lifelong digital literacy in mitigating online digital victimisation. This approach is suitable for drawing insights from existing research, identifying patterns, and generating theoretical and practical recommendations. This aligns with the broad thematic focus of this study analysing lifelong digital education as a long-term structural solution to cyber threats, which transcends immediate short-term interventions.

Data were collected from credible secondary sources, including peer-reviewed journal articles, academic books, institutional and government reports, policy documents, and program evaluations. Priority was given to sources that explicitly addressed digital literacy, lifelong learning, cybercrime, and crime-prevention strategies. Accordingly, a literature search was conducted through major academic

databases, including JSTOR, Scopus, and Google Scholar, supplemented by materials obtained from reputable institutions, such as UNESCO and the International Telecommunication Union (ITU). Combinations of keywords and search phrases were employed, including "digital literacy", "lifelong digital literacy", "digital competence", "lifelong learning", "online victimisation", "cyber victimisation", "cybercrime prevention", "cybersecurity awareness", "online safety", and "digital resilience". Searches were refined using Boolean operators, such as AND and OR, where appropriate. The literature search, completed in December 2025, covered publications from January 2005 to December 2025, with earlier seminal works included where necessary to establish the theoretical and conceptual foundations of the review. The search process initially identified approximately 170 records across all databases and institutions. After removing duplicate records, approximately 114 unique publications remained for screening. Following title, abstract, and full-text assessment for relevance, approximately 40 sources were retained for the final narrative synthesis.

Although this review did not follow the procedural requirements of a systematic review, efforts were made to ensure the relevance and quality of the consulted literature. Sources were selected based on their conceptual contribution to understanding the relationship between digital literacy and online victimisation, methodological rigor, and policy relevance. Studies were excluded if they were duplicates, lacked identifiable authorship or publication sources, were not available in English, focused primarily on unrelated forms of digital technology without addressing digital literacy or online victimisation, or did not make a meaningful conceptual, empirical, or policy contribution to the objectives of this review.

The collected materials were subjected to thematic analysis to identify recurring themes, gaps, and theoretical patterns in the literature. The retained literature was read iteratively and coded manually into broad thematic categories, including digital literacy competencies, online victimisation risks, cyber security awareness, lifelong learning approaches, behavioural change, institutional and policy interventions, and implications for online safety in Nigeria. These themes were subsequently synthesised to identify convergences, divergences, and knowledge gaps within the existing literature. Being well-suited for capturing broad societal trends and synthesising existing knowledge, this method allowed for the identification of underexplored areas in digital literacy research and policy while providing a theoretical foundation for future empirical work. The analytical process

was guided by Cohen and Felson's (1979) RAT and Bandura's (1977) SLT. These frameworks helped classify findings in relation to their explanatory power regarding cybercrime victimisation and the preventive role of digital literacy education. The RAT was used to assess how digital literacy functions as a form of guardianship, whereas the SLT aided in understanding how continuous digital education contributes to behavioural change and resilience.

To improve linguistic clarity, the manuscript underwent language editing using Grammarly, an artificial intelligence-assisted writing support tool. [insert hyperlink] The tool was used solely for editorial and language enhancements. All aspects of the study, including the research design, literature selection, analysis, interpretation of the findings, and conclusions were conducted and verified by the author.

Results and Discussion

In this section, the literature is thematically synthesised to examine the intersections between digital literacy and online victimisation. The synthesis draws on both Nigerian and international literature, with broader international findings interpreted in the Nigerian context where appropriate. The analytical process is grounded in RAT and SLT, which provide conceptual lenses for understanding how digital literacy can function as both a preventive mechanism and a behavioural resource in the digital age.

Vulnerable Populations and the Uneven Distribution of Digital Skills

The proliferation of digital technologies has created unprecedented opportunities for social, economic, and civic engagement. Consequently, digital literacy is increasingly recognised as a form of social capital essential for full participation in contemporary life. Digital literacy, as Hargittai (2010) emphasised, goes beyond mere access and includes the ability to evaluate information, manage privacy, and avoid deceptive content. However, these skills are less likely to be developed among individuals with limited exposure to formal or continuing education. Access to and proficiency in digital technologies are unevenly distributed across different population segments worldwide. This disparity, often referred to as the ‘digital divide’, disproportionately affects vulnerable populations who often lack access to devices, internet connectivity, and tailored educational opportunities (van Dijk,

2020). This results not only in technological exclusion but also in amplified socioeconomic disparities in the digital world. According to the ITU (2023), over 2.6 billion people remain offline, and even among those with Internet access, digital skill levels vary greatly. Although these statistics point to global trends, recent Nigerian evidence highlights persistent inequalities in digital access and skills (De Simone & Manolio, 2024).

From the perspective of RAT, these disparities have important implications for online victimisation. The theory posits that victimisation is more likely when a motivated offender encounters a suitable target in the absence of capable guardians. In digital environments, digital literacy can function as a form of capable guardianship by equipping individuals with the knowledge and skills necessary to identify phishing attempts, recognise fraudulent websites, evaluate the credibility of online information, manage privacy settings, and respond appropriately to cybersecurity threats. Individuals who lack these competencies are less able to detect and avoid online risks, thereby increasing their suitability as targets for cyber offenders. The reviewed literature suggests that limited digital literacy is associated with greater vulnerability to online fraud, identity theft, cyberbullying, and other forms of online victimisation (van Deursen & Helsper, 2015; Livingstone & Helsper, 2007). Thus, digital inequalities not only affect participation in the digital economy but also shape individuals' exposure to cybercrime risks.

SLT provides a complementary explanation for these vulnerabilities. According to Bandura (1977), behaviours and competencies are acquired through observation, imitation, social interaction, and reinforcement. Applied to digital environments, the theory suggests that individuals develop safe online practices through exposure to educational programs, peer networks, family members, workplace training, and other social learning contexts in which protective digital behaviours are demonstrated and reinforced. Vulnerable populations often have fewer opportunities to participate in such learning environments, reducing their exposure to positive digital role models and limiting their acquisition of effective cyber security behaviours. Consequently, they may be less likely to adopt practices such as strong password management, cautious information sharing, online source verification, and the use of security tools. The observed relationship between low digital literacy and heightened victimisation risk can, therefore, be understood not only as a consequence of limited technical skills but also as the outcome of unequal

access to social learning processes that facilitate the development of digital resilience.

Age is an important factor associated with digital inequality. Friemel (2016) found that older adults are less likely to engage with digital technologies because of cognitive, motivational, and socio-environmental barriers. Consequently, they are more vulnerable to cybercrimes, including phishing, financial scams and misinformation. In this vein, a systematic review by Choi and DiNitto (2013) indicates that older Internet users report less confidence in their ability to protect themselves online, which increases their susceptibility to cyberbullying. Low-income and low-education populations also face structural challenges in developing digital competence, although much of the available empirical evidence originates from studies conducted outside Nigeria. Helsper and van Deursen (2016) argue that socioeconomic status predicts not only access to digital devices but also the quality of digital engagement. Other vulnerable populations include women, rural dwellers, ethnic minorities, persons with disabilities, and people from the Global South (De Simone & Manolio, 2024). Public initiatives that aim to close the digital gap often fail to account for intersecting vulnerabilities such as poverty, language barriers, and limited institutional trust, leading to a continued skill divide even in connected regions. Intersectional approaches further reveal that digital skill disparities are not uniformly experienced by all the older adults. For example, women in rural or conservative contexts may face gendered restrictions on digital use, while ethnic minorities may encounter language barriers or systemic biases in technology design and deployment (Robinson et al., 2015).

Scholars have observed that the uneven distribution of digital skills significantly impacts individuals' abilities to detect, avoid, and recover from cyber threats (Fisk et al., 2022). For instance, Fischer et al. (2013) found that online fraud disproportionately affects older adults with low digital competence, partly due to their reduced capacity to identify scams and manage online privacy. Therefore, digital literacy is not only an educational concern but also a public safety priority. Promoting digital inclusion through lifelong learning is essential for achieving educational equity and cyber security resilience. Efforts to ensure this have led to a growing call for lifelong, culturally sensitive, linguistically accessible, and community-based digital-literacy intervention programs. In Nigeria, recent policy initiatives have recognised the importance of digital inclusion; however, targeted lifelong digital education for vulnerable populations remains comparatively limited

(Federal Ministry of Education, [FME] 2019; Federal Ministry of Communications and Digital Economy, [FMCDE], 2020). This policy gap reinforces structural inequalities and leaves large segments of the population vulnerable to digital harm, particularly children. Thus, without deliberate interventions, vulnerable individuals are likely to remain at a greater risk of digital exclusion and online victimisation in an increasingly digital world.

Lifelong Learning and Behavioural Adaptation in the Digital Environment

In today's hyperconnected world, the digital environment is not static; it is shaped by rapid innovations, shifting risks, and emerging social norms. Therefore, lifelong learning has emerged as a key strategy for enabling individuals to respond effectively to the evolving digital challenges. Although this perspective is largely informed by international scholarship, it is becoming increasingly relevant to Nigeria's expanding digital ecosystem. Defined as 'an organising principle for education that integrates formal, non-formal, and informal learning across the lifespan', lifelong learning involves not only acquiring technical know-how but also nurturing critical thinking, media literacy, ethical awareness, and adaptability to online risks (UIL, 2020). It also promotes flexible competencies that enable individuals to respond to rapid societal changes (Bélanger & Tuijnman (1997). Therefore, it is plausible to state that behavioural adaptation grounded in lifelong learning is highly relevant in digital settings, as it empowers citizens to engage safely, critically, and productively in online environments. This is because traditional once-in-a-lifetime digital training models are insufficient given the pace of technological change. Instead, individuals need to engage in ongoing re-skilling and up-skilling to adapt their behaviour as technologies evolve and cyber threats become increasingly sophisticated. This is particularly important in light of the "platformization" of everyday life, where people access banking, education, health services, and social interactions through digital platforms.

Bandura's (1977) SLT offers a useful framework for understanding how behavioural changes occur in digital environments. The theory posits that people learn new behaviours by observing others, especially when these behaviours are reinforced positively. In digital settings, learning occurs through interactions with peers, media content, online communities and digital mentors. As digital risks such as phishing, misinformation, and online fraud evolve, adaptive behaviours such as strong password use, critical evaluation of content, and cautious data sharing must

be constantly reinforced through accessible learning channels. In this light, digital literacy is not merely the acquisition of technical knowledge but a behavioural process through which individuals develop and internalise safe online practices. These behaviours can be acquired and refined through structured digital literacy interventions and informal learning mechanisms, such as online tutorials or peer guidance. Repeated exposure to cybersecurity awareness messages, demonstrations of safe online conduct, and positive reinforcement of protective behaviours can encourage the adoption and maintenance of practices that reduce vulnerability to cyber threats. Conversely, individuals who lack access to such learning opportunities may be less likely to acquire the competencies necessary for safe navigation of digital environments, thereby increasing their susceptibility to online victimisation.

Moreover, Merriam and Bierema (2014) emphasised the role of experiential learning in adult education, suggesting that adults are more likely to retain and apply digital safety practices when learning is contextual, problem-based, and iterative. Therefore, lifelong learning programs that foster reflection, engagement, and relevance are more likely to lead to meaningful behavioural adaptations. This insight complements SLT by highlighting how repeated engagement with real-world digital challenges reinforces learning and promotes behavioural adaptation. Therefore, lifelong learning programs that foster reflection, engagement, practical application, and relevance are more likely to facilitate the continuous development of digital competencies and strengthen individuals' resilience against emerging online threats.

Owing to its increasing relevance, lifelong digital education has transcended the status of a developmental goal and become imperative for public safety. As Kovács and Terták (2024) argued, individuals with limited and outdated digital and financial knowledge are disproportionately targeted by cybercriminals, while continuous learning often strengthens individuals' agency, enabling them to detect suspicious online behaviours, understand privacy settings, and report incidents more confidently. The socio-technical environment largely polarises digital behaviour along this divide. In other words, when users are empowered through regular exposure to updated knowledge and peer-to-peer learning, they are more likely to engage in protective behaviours and vice versa. For example, evidence from international studies suggests that users with higher digital literacy are less likely to fall for scams or cyberbullying attempts because of their proactive and

informed online behaviour (van Deursen & van Dijk, 2013). This shows that behavioural adaptation is both an outcome and a facilitator of lifelong learning, with individuals who embrace learning as an ongoing process being more open to modifying their behaviours, reflecting on past mistakes and incorporating safer practices into their daily routines.

Despite its promise, the implementation of lifelong digital learning faces several challenges. These include a lack of institutional coordination, limited access to inclusive learning opportunities, and the undervaluation of non-formal and informal learning channels. Furthermore, marginalised populations, such as the elderly, refugees, and low-income communities, are often excluded from digital upskilling initiatives. In light of these, coupled with the fact that behavioural change is not instantaneous, as it requires ongoing reinforcement through community education, government campaigns, employer training programs, and digital literacy embedded in healthcare, banking, and other service sectors (Livingstone & Helsper, 2007)—an integrated policy approach is needed to support behavioural change at scale, including within Nigeria's evolving digital education and cybersecurity policy landscape.

Digital Literacy as a Form of Guardianship Against Cybercrime

In the digital age, where cybercrime increasingly threatens personal safety, financial stability, and social trust, evidence suggests that digital literacy may serve as a protective mechanism against such threats. Beyond being a technical skill set, digital literacy enables individuals to critically assess information, recognise threats, and adopt preventive behaviours. This protective function aligns with the concept of ‘capable guardianship’ in the RAT, suggesting that digital literacy can serve as a form of informal social control that reduces the likelihood of online victimisation. This is because it tends to equip individuals with the knowledge and competencies required to identify, avoid, and respond to online threats before they cause harm. In other words, while users with low digital literacy often become "suitable targets" due to their inability to recognise phishing scams, data harvesting, or suspicious digital behaviour, individuals with high levels of digital literacy often act as their own guardians, deploying knowledge and skills to prevent victimisation. Therefore, the value of digital literacy extends beyond the acquisition of individual skills. It may function not only as a personal asset but also as a form of informal guardianship, decreasing the feasibility and success of cybercrimes. This reframing

of literacy as guardianship enhances the relevance of criminological theories in contemporary digital crime prevention discourse (Yar & Steinmetz, 2019).

To fully grasp the worth of digital literacy as a form of guardianship, it is necessary to state that it encompasses more than simply knowing how to use a computer or browse the web. As defined by the European Commission (2023), it includes the ability to access, manage, understand, integrate, communicate, evaluate, and create information safely and appropriately using digital technology. This broad competence framework provides individuals with the tools to protect themselves against fraud, misinformation, identity theft, cyberbullying, and ransomware attacks. Evidence from international studies indicates that individuals with low digital competence are more likely to fall victim to online scams and phishing emails (Hadlington, 2017). Conversely, those educated in digital hygiene—such as recognising secure websites, identifying suspicious links, and managing privacy settings—are more likely to resist online victimisation. Digital literacy thus has the potential to equip users to fulfil the role of capable guardians, mitigating the risk of criminal exploitation in cyberspace. It also contributes to community-level guardianship, as knowledgeable users share security tips, report suspicious activities, and guide peers. This collective effect creates informal guardianship networks that extend beyond the individual, strengthening digital resilience at the societal level (Wall, 2007).

However, the protective potential of digital literacy varies across demographic groups, with vulnerable populations having a lesser ability to serve as communities or even as self-guardians of their health. For instance, older adults are often less digitally literate and, thus, more susceptible to cyber threats. Targeted digital literacy training may strengthen their ability to act as capable guardians online, particularly when complemented by appropriate technical, institutional, and social support measures. Children and adolescents are another example of vulnerable populations that require support to develop digital competencies. Although they are often digitally fluent, they lack critical thinking skills and risk awareness, thus requiring contextualised education that goes beyond basic skills. Without proactive interventions, these groups will remain excluded from digital guardianship and thus become prime targets for cybercrimes (Van Deursen & van Dijk, 2013). Therefore, public policies that integrate digital literacy into national security strategies, adult education, and community outreach programs are essential. In this vein, the Organization for Economic Co-operation and Development (OECD, 2021)

reiterated that collaborative models involving governments, Non-Governmental Organizations (NGOs), and private tech companies can help deliver sustainable, context-sensitive digital literacy programs that foster long-term guardianship across diverse populations. Although this recommendation is derived from international policy experience, it offers useful guidance for strengthening digital inclusion and online safety initiatives in Nigeria. However, scholars have argued that digitalising public administration can support the advancement of digital governance and facilitate the implementation of such initiatives in Nigeria (Mshelia & Kari, 2024; Kari & Mshelia, 2023).

Limitations of Current Digital Literacy Initiatives

Despite growing global awareness of the importance of digital literacy, current initiatives often fall short of addressing the full scope and diversity of users' needs, especially among vulnerable populations. These shortcomings are not only global but are also acutely felt in Nigeria, where digital literacy disparities intersect with systemic challenges in education, infrastructure and governance.

Globally, many digital literacy programs focus predominantly on children and youth through formal educational institutions. This approach assumes that digital competence developed early in life is maintained throughout adulthood. However, this excludes significant demographics, including adults, the elderly, and those outside traditional education systems. In Nigeria, this youth-focused model is reinforced through initiatives such as the *National Digital Economy Policy and Strategy (2020–2030)*, which emphasises ICT integration in schools and universities (FMCDE, 2020). Others include the *National Policy on Information and Communication Technologies in Education (NPICTIE)* and the *National Implementation Guidelines for ICT in Education (NIGICTIE)* launched in 2019 (FME, 2019). While important, these initiatives provide comparatively fewer structured digital learning opportunities for older adults, informal sector workers and rural dwellers, potentially increasing their vulnerability to cybercrime.

While the OECD (2021) emphasised the need for integrated national strategies that align education, technology, and crime prevention, such alignment remains nascent in many countries, weakening the institutionalisation of digital literacy as a preventive strategy for cybercrime. For example, in Nigeria, digital literacy programs suffer from fragmentation, a lack of coordination, and uneven distribution. Available evidence suggests that many digital literacy projects are

donor-funded or NGO-led with limited sustainability, thus lacking integration into national education and security policy frameworks. For example, while programs like the *Digital Literacy for All Initiative* aim to bridge access gaps, they often operate in silos, with insufficient coordination between the education sector, cybersecurity agencies, and local governments.

Limited curriculum scope and cultural relevance are other challenges confronting digital literacy initiatives. Most digital literacy programs—globally and in Nigeria—focus on basic technical skills such as typing, Internet browsing, or using productivity tools. These are insufficient in an age where cyber threats involve complex schemes such as phishing, identity theft, ransomware, and digital misinformation. Ng (2012) stressed that digital literacy should include critical thinking, media literacy, and cyber security awareness. In Nigeria, cultural and linguistic diversity poses additional challenges to curriculum designs. Digital education materials are often in English, which automatically limits access for those with low English literacy. Additionally, local relevance is often overlooked, as many global training programs are poorly adapted to the socioeconomic realities of informal economies or rural life in the country. Gender disparities persist in some parts of the country. For instance, women and girls in parts of northern Nigeria face cultural barriers to education, including digital education (Centre for Information Technology and Development, 2021; De Simone & Manolio, 2024).

Other challenges confronting digital initiatives in Nigeria include governance constraints, insecurity, and institutional inefficiencies that may hinder programme implementation (Mshelia & Kari, 2024). These converge to create structural barriers to access, socioeconomic disparities, infrastructural gaps, and urban-rural divides, all of which significantly hinder access to digital literacy training in the country. For example, while Van Dijk (2020) highlighted the role of material access in perpetuating digital inequality, Sasu (2024) revealed that only approximately 50% of Nigerians have Internet access, with rural Internet penetration significantly lower than in urban areas. This is exacerbated by insufficient evaluation and long-term impact assessment which is essential for policy feedback and program design but remains underutilised in both national and NGO-led initiatives in the country. Available evaluations of digital literacy programmes in Nigeria seldom assess long-term behavioural changes or changes in vulnerability to online victimisation. Program assessments are often absent, anecdotal, or donor-driven, with limited transparency and academic scrutiny. This lack of evaluation restricts learning and

scalability because without disaggregated data (by age, gender, and region), it is difficult to track progress, understand effectiveness, or tailor programs to diverse contexts.

Conclusion and Recommendations

Digital literacy is not just about navigating technology but also about safeguarding human rights, fostering inclusion and enhancing public safety in an increasingly digital world. This study explored the potential of lifelong digital literacy in reducing vulnerability to online victimisation, with particular attention to vulnerable populations and systemic limitations of existing initiatives. Vulnerable populations, such as older adults, rural dwellers, women, and those with limited formal education, are disproportionately affected by the digital divide and face heightened exposure to online risks because of their limited digital skills. The reviewed evidence suggests that lifelong digital literacy can support behavioural adaptation to evolving cyber threats. Viewing through the analytical lens of RAT, it is a form of guardianship that helps individuals identify threats and reduce their likelihood of being suitable targets for online offenders, informing the need to see it as not merely a one-time educational achievement but a continuous protective process. Drawing on both international evidence and emerging Nigerian experience, lifelong, inclusive, and context-sensitive digital education should become an important component of educational and security systems in vulnerable contexts, such as Nigeria.

Available evidence suggests that many digital literacy programmes in Nigeria remain fragmented, under-resourced, and insufficiently targeted, with significant gaps in content relevance, access equity, and programme evaluation. These structural and strategic challenges are compounded by infrastructural deficits, social inequality and fragmented policy environments. While some progress has been made through ICT integration in schools and donor-supported training projects, significant gaps remain in reaching older adults, marginalised groups and the rural poor. To move forward, Nigeria needs to embed digital literacy in broader lifelong learning and national crime prevention strategies, localise content to match linguistic, cultural, and economic contexts, develop inclusive multi-stakeholder frameworks that engage federal, state, and community actors, and implement robust evaluation systems to guide evidence-based improvement. Such integrated, inclusive, and adaptive approaches have the potential to strengthen the contribution

of digital literacy to online safety and cybercrime prevention in Nigeria. In light of this, the following specific recommendations are proposed:

1. Governments and stakeholders should embed digital literacy into lifelong learning frameworks that extend beyond the classroom in pursuit of a mission that views digital education as a civic necessity, not a privilege. This should include the establishment and strengthening of existing adult education centres, vocational training institutions, public libraries, and online platforms accessible to all age groups.

2. Digital literacy interventions should be explicitly tailored to meet the needs of vulnerable populations. Programs should be designed with sensitivity to local languages, cultural contexts, and literacy levels. Special efforts should be made to include vulnerable populations in both the design and delivery phases.

3. Policymakers should formally recognise digital literacy as a non-technical security measure and integrate it into broader crime prevention strategies. The inclusion of criminological frameworks, such as the RAT, can help policymakers understand digital education as a proactive tool against online victimisation.

4. Training materials should be developed to reflect local realities, including popular scams, local digital practices, and region-specific threats. Partnerships between cybersecurity experts, educators, community leaders, and civil society organisations should be leveraged to enhance curriculum relevance and impact.

5. Given the infrastructural limitations in many parts of Nigeria and other Global South countries, community-based models, such as mobile digital clinics, rural digital hubs, and radio-based education, should be explored to widen access to mental health services. Community champions and peer-learning structures should be utilised to aid information diffusion.

6. Robust mechanisms should be established to evaluate the impact of digital literacy programmes on the elderly. The evaluation should be disaggregated by age, gender, location, and income level to ensure equity and continuous improvements. The lessons learned should be directly incorporated into policy refinement and program redesign.

Declaration of Interest Statement

The author declares no conflict of interest concerning this manuscript.

Funding Statement

This study did not receive any specific grants from any funding agency in the public, commercial, or non-profit sectors. The study was conducted independently by the author as part of their academic research activities.

References

Abdullah, M., Nawaz, M. M., Saleem, B., Zahra, M., Ashfaq, E. B., & Muhammad, Z. (2025). Evolution cybercrime Key trends, cybersecurity threats, and mitigation strategies from historical data. *Analytics*, *4*(3), 25. https://doi.org/10.3390/analytics4030025

American Library Association. (2011). *Digital literacy, libraries, and public policy: Report of the Office for Information Technology Policy's digital literacy task force*. https://alair.ala.org/bitstreams/db72e923-1e14-45b8-ab0e-b113241c0e4c/download

Ani, J. I., & Batisai, K. (2024). Promoting digital inclusion through public-private partnerships for older adults in Nigeria: A review. *Aging and Health Research*, *4*(4), 100211. https://doi.org/10.1016/j.ahr.2024.100211

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

Bélanger, P., & Tuijnman, A. (1997). *New patterns of adult learning: A six-country comparative study* (1st ed.). Pergamon; UNESCO Institute for Education.

Centre for Information Technology and Development. (2021). *Internet for men? The digital marginalization of women in northern Nigeria*. https://www.citad.org/wp-content/uploads/2021/07/INTERNET-FOR-MEN-The-Digital-Marginalisation-of-women-in-Northern-Nigeria.pdf

Choi, N. G., & DiNitto, D. M. (2013). Internet use among older adults: Association with health needs, psychological capital, and social capital. *Journal of Medical Internet Research*, *15*(5), e97. https://doi.org/10.2196/jmir.2333

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588–608. https://doi.org/10.2307/2094589

De Simone, M. E., & Manolio, F. A. (2024). *Digital skills in Nigeria: A summary of the population's skills and the availability of digital infrastructure in schools*. World Bank Group. http://documents.worldbank.org/curated/en/099954107182514013

European Commission. (2023). *Digital education action plan (2021–2027): Resetting education and training for the digital age*. https://education.ec.europa.eu/focus-topics/digital-education/action-plan

Federal Ministry of Communications and Digital Economy. (2020). *National digital economy policy and strategy (2020–2030).*

Federal Ministry of Education. (2019). *National policy on information and communication technologies (ICT) in education*. http://education.gov.ng/wp-content/uploads/2019/08/NATIONAL-POLICY-ON-ICT-IN-EDUCATION-2019.pdf

Fischer, P., Lea, S. E., & Evans, K. M. (2013). Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. *Journal of Applied Social Psychology*, *43*(10), 2060–2072. https://doi.org/10.1111/jasp.12158

Fisk, R. P., Gallan, A. S., Joubert, A. M., Beekhuyzen, J., Cheung, L., & Russell-Bennett, R. (2022). Healing the digital divide with digital inclusion: Enabling human capabilities. *Journal of Service Research*, *26*(4), 542–559. https://doi.org/10.1177/10946705221140148

Friemel, T. N. (2016). The digital divide has grown old: Determinants of a digital divide among seniors. *New Media & Society*, *18*(2), 313–331. https://doi.org/10.1177/1461444814538648

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon*, *3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hargittai, E. (2010). Digital na(t)ives? Variation in internet skills and uses among members of the "net generation." *Sociological Inquiry*, *80*(1), 92–113. https://doi.org/10.1111/j.1475-682X.2009.00317.x

Helsper, E. J., & van Deursen, A. J. A. M. (2016). Do the rich get digitally richer? Quantity and quality of support for digital engagement. *Information, Communication & Society*, *20*(5), 700–714. https://doi.org/10.1080/1369118X.2016.1203454

International Telecommunication Union. (2023). *Facts and figures 2023: Measuring digital development*. https://www.itu.int/hub/publication/d-ind-ict_mdd-2023-1/

Kari, A. G. U., & Mshelia, I. H. (2023). Digitalising public administration for sustainable development: The Nigerian experience. *Digital Policy Studies*, *2*(1), 32–50. https://doi.org/10.36615/dps.v2i1.2708

Kovács, L., & Terták, E. (2024). Financial literacy is the best protection from cybercrime. *Economy and Finance*, *11*(1), 7–28. https://doi.org/10.33908/EF.2024.1.2

Livingstone, S., & Helsper, E. J. (2007). Gradations in digital inclusion: Children, young people and the digital divide. *New Media & Society*, *9*(4), 671–696. https://doi.org/10.1177/1461444807080335

Merriam, S. B., & Bierema, L. L. (2014). *Adult learning: Linking theory and practice*. Jossey-Bass. https://download.e-bookshelf.de/download/0003/9722/52/L-G-0003972252-0002483324.pdf

Mitchell, K. J., Finkelhor, D., Wolak, J., Ybarra, M. L., & Turner, H. (2011). Youth Internet victimization in a broader victimization context. *The Journal of Adolescent Health*, *48*(2), 128–134. https://doi.org/10.1016/j.jadohealth.2010.06.009

Mshelia, I. H., & Kari, A. G. U. (2024). Digital governance: A pathway for combating emerging public safety and security challenges in 21st century Nigeria. *Society and Security Insights*, *7*(2), 47–68. https://doi.org/10.14258/ssi(2024)2-03

National Academies of Sciences, Engineering, and Medicine. (2025). *Cybercrime classification and measurement: Consensus study report highlights*. National Academies Press. https://nap.nationalacademies.org/resource/29048/Highlights_Cybercrime_Classification_and_Measurement.pdf

Ng, W. (2012). Can we teach digital natives digital literacy? *Computers & Education*, *59*(3), 1065–1078. https://doi.org/10.1016/j.compedu.2012.04.016

OECD. (2021). *21st-century readers: Developing literacy skills in a digital world*. OECD Publishing. https://doi.org/10.1787/a83d84cb-en

Robinson, L., Cotten, S. R., Ono, H., Quan-Haase, A., Mesch, G., Chen, W., Schulz, J., Hale, T. M., & Stern, M. J. (2015). Digital inequalities and why they matter. *Information, Communication & Society*, *18*(5), 569–582. https://doi.org/10.1080/1369118X.2015.1012532

Sasu, D. D. (2024, October 1). *Number of internet users in Nigeria 2017–2024*. Statista. https://www.statista.com/statistics/1176087/number-of-internet-users-nigeria/

UNESCO Institute for Lifelong Learning. (2020). *Embracing a culture of lifelong learning: Contribution to the Futures of Education initiative. Report: A*

transdisciplinary expert consultation. https://unesdoc.unesco.org/ark:/48223/pf0000374112

UNESCO Institute for Lifelong Learning. (2022). *Chapter 1: Introducing lifelong learning—1.1 Defining lifelong learning. Lifelong Learning e-Toolkit*. https://lifelonglearning-toolkit.uil.unesco.org/en/node/177

van Deursen, A. J. A. M., & Helsper, E. J. (2015). The third-level digital divide: Who benefits most from being online? *Communication and Information Technologies Annual*, *10*, 29–52. https://doi.org/10.1108/S2050-206020150000010002

van Deursen, A. J., & van Dijk, J. A. (2013). The digital divide shifts to differences in usage. *New Media & Society*, *16*(3), 507–526. https://doi.org/10.1177/1461444813487959

van Dijk, J. A. G. M. (2020). *The digital divide*. Polity Press.

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The digital competence framework for citizens: With new examples of knowledge, skills and attitudes* (JRC128415). Publications Office of the European Union. https://doi.org/10.2760/115376

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity. https://ssrn.com/abstract=1066922

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society* (2nd ed.). Sage.

Appendix I

Schematic of a Proposed Classification of Cybercrime

Category	Illustrative sub-categories/examples	Level of cyber (computer) involvement
Acts targeted against machines, data, or systems	Ransomware Unlawful access or deprivation of access like cyber trespass and denial-of-service attacks Unlawful interference, tampering, or content release like hacking, destructive malware, unlawful data breaches. Other acts targeted against machines, data, or systems	Cyber-dependent = high cyber involvement
Fraud and acts targeted against property	Identity theft including elements of both unlawful acquisition of personal information (theft) and	Cyber-enabled = moderate cyber involvement

	misuse of that information to commit fraud (e.g., abuse existing account or create new account). Fraud like phishing, swindles and confidence game. Other acts targeted against property	
Acts against individuals, nonsexual in nature	Cyber harassment, cyberstalking, cyberbullying	Cyber-enabled = moderate cyber involvement
Acts against individuals, sexual in nature	Unlawful sexual exploitation material via electronic means	Cyber-enabled = moderate cyber involvement
Acts targeted against groups	Computer-related acts of terrorism or radicalization.	Cyber-enabled = moderate cyber involvement
Acts involving incidental technology use	Using information and communication technology (ICT) to lure a victim into a physical attack	Cyber-assisted = low cyber involvement

Note. Adapted from Cybercrime Classification and Measurement: Consensus Study Report Highlights (p. 2), by National Academies of Sciences, Engineering, and Medicine (2025), National Academies Press. https://nap.nationalacademies.org/resource/29048/Highlights_Cybercrime_Classification_and_Measurement.pdf