THE ROLE OF PUBLIC AWARENESS AND DIGITAL LITERACY IN PREVENTING CYBERCRIME IN NIGERIA

Goodluck ETINAGBEDIA, Ph.D.,
Delta State University, Abraka
etinagbediagoodluck97@gmail.com

Abstract: *Cybercrime has become a significant threat to Nigeria's national security, economic well-being, and individual privacy. With the nation's rapid digital advancement and increased dependence on online platforms, citizens are increasingly exposed to cyber threats such as phishing, identity theft, and online financial scams. This study, therefore, explored how public awareness and digital literacy serve as preventive measures against cybercrime in Nigeria. Utilizing a historical research approach, the study analyzed data from government publications, scholarly journal articles, and media reports over the last twenty years to chart the development of cyber threats and the efforts made to address them. Anchored on Social Learning Theory, which emphasizes that individuals acquire behaviours through observation and education, the study highlights how improved digital knowledge and skills could help reduce risky online practices and cybercrime victimization. The findings indicated that, despite efforts by institutions like the Nigerian Communications Commission (NCC) and the Economic and Financial Crimes Commission (EFCC) to promote cybersecurity awareness, substantial gaps in digital literacy remain, especially in rural communities and among young people. The study concluded that promoting public awareness and building digital capacity are essential for long-term cybercrime prevention. It recommended, among others, that the Nigerian government should embed digital literacy into school curricula from primary to tertiary levels. Beyond basic ICT, students should learn cybersecurity essentials such as safe browsing, password protection, and online privacy. Teaching these skills early will prepare young people to engage safely and confidently in the digital world.*

Keywords: *cybercrime; public awareness; digital literacy; social learning theory; Nigeria.*

Introduction

The swift growth of information and communication technologies (ICTs) has reshaped the global environment, offering new possibilities for creativity, interaction, and socio-economic progress. Like many other nations, Nigeria has embraced this digital shift, with millions of people now connected through smartphones, internet services, and social media platforms. Yet, alongside these benefits in access to information, business, and governance, has come a surge in cyber threats targeting individuals, organizations, and even the state (Audu et al., 2023). Cybercrime has become a critical concern in Nigeria, ranging from phishing, identity theft, and hacking to ransomware, online fraud, and advanced financial crimes that erode trust in digital systems.

Promoting public awareness and digital literacy has therefore become vital in addressing these challenges. Technology and legal measures alone are insufficient; human knowledge and vigilance remain central to prevention. Citizens who are digitally literate are more capable of detecting suspicious online activities, safeguarding personal data, and practicing safe internet habits. In Nigeria, where criminal networks such as the so-called "Yahoo Boys" have gained global attention, the urgency for grassroots sensitization and structured digital education is more pronounced (Okeshola & Adeta, 2022). The extent to which people understand and apply digital knowledge directly affects both their online behaviour and their vulnerability to cybercrime.

The Nigerian government, in collaboration with private sector stakeholders, has introduced several measures to enhance cybersecurity, including the Cybercrime (Prohibition, Prevention, Etc.) Act of 2015. However, the persistence of cybercrime indicates that legal enforcement alone is inadequate. Researchers argue that awareness campaigns, training programs, and the integration of digital literacy into school systems are necessary complementary measures (Eze & Eze, 2021). Digital literacy extends beyond technical ability; it also involves the capacity to critically evaluate information, recognize threats, and engage responsibly in online spaces.

On the global scale, evidence suggests that countries with higher digital literacy levels experience lower rates of cybercrime, as their citizens are empowered to actively protect themselves (Igbinedion & Aladenusi, 2022). In Nigeria, however, gaps in internet safety education, socio-economic disparities, and weak awareness structures continue to expose large sections of the population. Groups such as students, rural residents, and small business operators are especially at risk because they rely heavily on online platforms without sufficient cyber safety knowledge (Obi & Osho, 2023). Combating cybercrime in Nigeria, therefore, requires more than the efforts of experts or government agencies; it must involve citizens who are informed, vigilant, and proactive.

This study is significant because it explores how public awareness, and digital literacy can act as preventive strategies in Nigeria's battle against cybercrime. It contributes to broader discussions on sustainable cyber governance in Africa by highlighting how digital competence and awareness shape resilience.

Conceptual Review

Cybercrime

Cybercrime refers to unlawful acts committed through computers, digital networks, or internet-enabled devices. It covers a broad spectrum of offenses, such as phishing, identity theft, hacking, cyberbullying, ransomware, online scams, and the spread of harmful software. Researchers point out that cybercrime is distinct from traditional crime because it transcends borders, occurs at a faster pace, and can cause widespread damage (Ndukwe & Okoli, 2022). In Nigeria, this issue has become particularly pronounced due to the activities of online fraudsters popularly known as "Yahoo Boys," who target both domestic and foreign victims (Audu, Nwogu, & Afolabi, 2023).

The growth of Nigeria's digital economy has also created more opportunities for cybercriminals. While online banking, e-commerce, and mobile money services have boosted convenience and financial inclusion, they have also increased exposure to cyber risks (Obi & Osho, 2023). The impact of cybercrime is not only financial; it erodes public trust in digital systems, discourages investments, and damages the country's reputation. Between 2019 and 2022, cyber fraud was estimated to cost Nigeria about $500 million annually, underscoring its seriousness as both an economic and security challenge (Okeshola & Adeta, 2022).

From a criminological perspective, the Routine Activity Theory explains that cybercrime thrives when three elements align: motivated offenders, suitable targets, and the absence of effective guardians in cyberspace (Cohen & Felson, 1979; revised in Ajayi, 2021). Therefore, tackling cybercrime requires not only focusing on perpetrators but also addressing the awareness, attitudes, and behaviours of potential victims. This makes public awareness and digital literacy essential in reducing cyber risks in Nigeria.

Public Awareness

Public awareness is the extent to which people understand and are conscious of specific issues, in this case, cybercrime and cybersecurity. It refers to what individuals know about online threats, the tactics used by cybercriminals, and the available methods to protect themselves (Eze & Eze, 2021). Awareness is active; it shapes how individuals think and act in terms of safe online practices.

In cybersecurity, awareness means being able to identify suspicious messages, avoid unsafe websites, use strong passwords, and understand the dangers of oversharing personal details. Agencies such as the Nigerian Communications Commission (NCC) and the Economic and Financial Crimes Commission (EFCC) have run public campaigns to educate people on phishing scams and fraudulent online investment schemes (Igbinedion & Aladenusi, 2022).

Studies indicate that cybercrime flourishes in contexts where citizens lack adequate knowledge of online risks (Obi & Osho, 2023). Populations that are not well-informed become easy targets. Awareness initiatives, therefore, are preventive measures that empower individuals and organizations to recognize, avoid, and report suspicious activities. At the same time, awareness efforts contribute to building a culture of vigilance that enhances national security.

It is important to note that awareness is context-driven. In Nigeria, social inequality, language diversity, and low literacy levels influence how people engage with cybersecurity campaigns (Okeshola & Adeta, 2022). For awareness strategies to work effectively, they must be inclusive, available in local languages, and tailored to vulnerable groups such as students, small-scale entrepreneurs, and rural residents.

Digital Literacy

Digital literacy goes beyond knowing how to use computers—it is the ability to apply digital tools safely, critically evaluate online information, and act responsibly in the digital world. According to UNESCO (2022), digital literacy involves skills such as information management, communication, collaboration, critical thinking, problem-solving, and ethical digital behaviour. It equips individuals to navigate online environments wisely, seizing opportunities while avoiding risks.

In cybersecurity terms, digital literacy acts as a shield. A digitally literate person not only uses online platforms effectively but also knows how to safeguard data, recognize phishing attempts, prevent malware infections, and adopt protective practices like two-factor authentication (Audu et al., 2023). However, in Nigeria, digital literacy is unevenly distributed. People in cities generally have more exposure and access to ICT training compared to those in rural areas (Ndukwe & Okoli, 2022).

Increasingly, digital literacy is recognized as an element of digital citizenship. It provides individuals with the skills and ethical responsibility to act as safe, active, and responsible participants in the digital economy. Programs like the Federal Ministry of Communications and Digital Economy's "Digital Nigeria" initiative aim to train citizens in basic cybersecurity, coding, and safe digital habits (Eze & Eze, 2021).

Moreover, digital literacy is not fixed. As cybercriminals develop new methods, ongoing learning becomes crucial. This highlights the importance of integrating digital literacy into Nigeria's school curriculum and workplace training programs. Without it, individuals remain vulnerable even in the presence of strong cybersecurity laws.

Understanding Cybercrime in Nigeria

Nigeria's digital economy has expanded rapidly in recent years, fueled by wider access to mobile phones, cheaper internet services, and a thriving technology sector. This growth has boosted economic activities, improved governance processes, and enhanced social connectivity. However, it has also created more avenues for cybercrime, including phishing, identity theft, ransomware, and online fraud (Audu, Nwogu, & Afolabi, 2023). The rise of internet fraudsters, commonly referred to as "Yahoo Boys," has further damaged Nigeria's reputation, as their schemes target victims both within the country and abroad (Ndukwe & Okoli, 2022). Although the Cybercrime (Prohibition, Prevention, etc.) Act of 2015 was enacted to deter offenders, legislation and enforcement alone have not been enough. A major factor often overlooked is the role of human behaviour, especially the need for stronger public awareness and digital literacy as preventive strategies.

Cybercrime describes unlawful acts carried out through digital platforms, networks, or computer systems. Unlike conventional crimes, it is transnational, swift, and capable of inflicting widespread damage (Ajayi, 2021). In Nigeria, common examples include hacking, phishing, cyberbullying, and ransomware (Obi & Osho, 2023). Between 2019 and 2022, cyber fraud was estimated to cost the country about $500 million annually, underscoring its serious economic and security implications (Okeshola & Adeta, 2022). Beyond financial harm, cybercrime also reduces trust in digital platforms, discourages foreign investment, and damages Nigeria's global standing.

Routine Activity Theory provides insight into these developments. It suggests that crime takes place when motivated offenders, suitable targets, and the absence of capable guardians coincides (Cohen & Felson, 1979). In Nigeria's digital space, the rapid growth of online activity has created abundant targets, while inadequate awareness and limited digital literacy leave citizens vulnerable (Ajayi, 2021). This makes it clear that cybercrime prevention cannot rely only on law enforcement; it must also focus on equipping citizens with the knowledge and skills to defend themselves online.

Public Awareness and Its Role in Preventing Cybercrime

Public awareness is the extent to which people understand the risks of cybercrime and the measures needed for protection (Eze & Eze, 2021). It shapes how individuals view online threats and influences their response to them. Informed citizens are far less likely to be deceived by fraudulent emails, malicious websites, or internet scams.

In Nigeria, agencies like the Nigerian Communications Commission (NCC) and the Economic and Financial Crimes Commission (EFCC) have initiated campaigns to inform the public about cyber risks. These programs highlight safe practices such as identifying phishing scams, protecting personal information, and reporting suspicious incidents (Igbinedion & Aladenusi, 2022). Nonetheless, knowledge gaps persist, particularly across different social and educational groups.

Studies show that a lack of awareness increases the chances of victimization (Obi & Osho, 2023). Many Nigerians still use weak passwords, overshare sensitive information, and engage in risky online behaviour. Well-designed awareness initiatives can therefore act as preventive measures by empowering citizens to serve as their own first line of defense.

However, awareness strategies must be inclusive and context sensitive. Nigeria's social and economic inequalities, language diversity, and varying levels of education affect how citizens interpret cybersecurity messages (Okeshola & Adeta, 2022). To be effective, campaigns should be localized, delivered in different languages, and tailored to vulnerable groups such as rural dwellers, students, and small business owners.

Digital Literacy as a Cybersecurity Tool

Digital literacy involves more than the ability to use a computer. It is the capacity to navigate digital environments responsibly, critically evaluate online content, and adopt safe practices when using technology (UNESCO, 2022). It includes skills such as information management, digital communication, online ethics, and cybersecurity habits.

A digitally literate individual in Nigeria can detect suspicious links, avoid unsafe websites, enable two-factor authentication, and secure personal data. In this way, digital literacy provides not only functional ICT skills but also the defensive knowledge necessary to reduce exposure to cyber threats (Audu et al., 2023).

The Nigerian government has acknowledged this need through programs like “Digital Nigeria,” which trains citizens in coding, cybersecurity awareness, and responsible online participation (Eze & Eze, 2021). Still, digital divide persists, urban populations typically have better access to ICT infrastructure and training than rural communities (Ndukwe & Okoli, 2022).

Embedding digital literacy into Nigeria’s education system and workplace training is therefore essential. Schools should integrate cybersecurity into curricula, while organizations should ensure ongoing training for employees. Given the constant evolution of cybercrime techniques, digital literacy must be continuously updated to remain effective.

Interrelationship Between Awareness, Digital Literacy, and Cybercrime Prevention

Cybercrime, public awareness, and digital literacy are deeply interconnected in influencing the safety of individuals and societies in today’s digital world. Cybercrime constitutes the central threat, often taking the form of online fraud, phishing attacks, hacking, identity theft, and ransomware. Public awareness determines how people identify and interpret these dangers, while digital literacy equips them with the technical abilities required to protect themselves and respond effectively. When citizens possess both awareness and digital competence, their chances of falling victim to cybercriminals are greatly reduced. Research evidence indicates that societies with widespread awareness initiatives and higher levels of digital literacy tend to record significantly lower cybercrime rates (Obi & Osho, 2023; Audu, Nwogu, & Afolabi, 2023).

In Nigeria, however, cybercrime continues to thrive despite the existence of legal frameworks such as the Cybercrime (Prohibition, Prevention, Etc.) Act of 2015. This persistence underscores a fundamental gap in human capacity. Awareness alone may result in individuals who recognize cyber risks but lack the skills to protect themselves, while literacy without awareness produces technically skilled individuals who remain vulnerable because they are unaware of evolving online threats (Okeshola & Adeta, 2022; Ndukwe & Okoli, 2022). Consequently, addressing Nigeria’s cybercrime challenge requires an integrated strategy that combines both awareness and literacy (Eze & Eze, 2021).

Beyond individual protection, awareness and digital literacy generate ripple effects within communities. Digitally literate and informed individuals often become agents of knowledge transfer, sharing cybersecurity practices with their peers, relatives, and colleagues. This peer-to-peer dissemination builds collective resilience against cybercrime. For example, university students who undergo cybersecurity training frequently share their knowledge with classmates, while small business owners trained in secure digital practices often extend these insights to their customer base and professional networks (UNESCO, 2022; Igbinedion & Aladenusi, 2022).

Community-based learning strategies have proven especially effective in Nigeria, where cultural and social contexts influence how information is received and applied. Campaigns delivered in local languages or targeted training workshops for rural dwellers help bridge inequalities in education and technology access. Such grassroots-focused interventions ensure that vulnerable groups, including women, students, and low-income entrepreneurs gain the knowledge and skills required to navigate the digital environment safely, thereby strengthening the country's resilience against cyber threats (Obi & Osho, 2023; Audu et al., 2023).

In conclusion, cybercrime flourishes where public awareness and digital literacy are underdeveloped. However, prevention becomes significantly more effective when both are integrated. Awareness shapes perceptions of risk, while digital literacy equips individuals with technical tools to act on those perceptions. Together, they nurture a culture of vigilance and responsible digital behavior. When multiplied across communities, these elements not only reduce the likelihood of cybercrime victimization but also enhance public trust in Nigeria's digital economy, ultimately supporting broader goals of national development (Eze & Eze, 2021; UNESCO, 2022).

Challenges in Leveraging Public Awareness and Digital Literacy for Cybercrime Prevention in Nigeria

Despite notable progress in digital transformation and the launch of several awareness initiatives, Nigeria still struggles to effectively harness public awareness and digital literacy as long-term strategies for reducing cybercrime. The challenges include:

1. Limited Reach of Awareness Campaigns: Most cybersecurity sensitization efforts in Nigeria are heavily concentrated in major urban areas such as Lagos, Abuja, and Port Harcourt, where internet penetration and ICT facilities are relatively better. Unfortunately, rural communities, home to a significant portion of the population, are often left out. This imbalance results in unequal access to cybersecurity knowledge, leaving rural dwellers more exposed to online scams and fraud. As Igbinedion and Aladenusi (2022) observe, campaigns that neglect rural populations deepen the digital divide and weaken national resilience against cyber threats.

2. Inadequate ICT Infrastructure: A key barrier to digital literacy is Nigeria's uneven ICT infrastructure. Many rural and semi-urban areas suffer from poor internet connectivity, unstable electricity supply, and high data costs. UNESCO (2022) stresses that digital literacy cannot thrive in contexts where affordable internet and reliable devices are lacking. This infrastructural gap prevents large segments of the population from acquiring essential cybersecurity skills, thereby increasing their vulnerability (Audu, Nwogu, & Afolabi, 2023).

3. Low Funding and Policy Gaps: Cybersecurity education and awareness are frequently treated as short-term projects rather than institutionalized, long-term policies. Government funding for such initiatives is inconsistent, and collaboration between relevant agencies such as the Nigerian Communications Commission (NCC) and the Economic and Financial Crimes Commission (EFCC) is often weak. Okeshola and Adeta (2022) argue that without consistent funding and well-coordinated frameworks, awareness campaigns risk being reactive, focusing on immediate threats rather than long-term prevention. Similarly, Eze and Eze (2021) note that cybercrime prevention is often underfunded when compared to other policy priorities, making it difficult to sustain community-level interventions.

4. Cultural and Language Barriers: The effectiveness of awareness campaigns is further hindered by linguistic and cultural factors. Since most campaigns are conducted in English, large sections of the population, especially those in rural areas with limited formal education, remain excluded. This reduces the overall impact of cybersecurity messages, as many citizens fail to grasp the risks or the preventive measures being promoted. Ndukwe and Okoli (2022) suggest that adopting indigenous languages and culturally relevant methods of communication, such as local radio broadcasts, drama, and town-hall meetings, would significantly improve reach and effectiveness. These localized approaches ensure that even vulnerable populations can actively participate in cybercrime prevention.

5. Rapid Evolution of Cybercrime: Cybercrime in Nigeria continues to evolve at a pace faster than most awareness and literacy campaigns can adapt to. Criminals regularly change tactics, from phishing and identity theft to more sophisticated schemes involving cryptocurrency fraud and deepfake technologies. Obi and Osho (2023) note that this constant evolution undermines the effectiveness of existing programs, as many citizens remain unprepared for emerging threats. To remain relevant, awareness and literacy programs must be continuously updated and informed by real-time intelligence and global best practices.

Thus, while Nigeria has made commendable efforts in promoting digital awareness and literacy, persistent obstacles such as uneven campaign coverage, poor ICT infrastructure, inadequate funding, cultural barriers, and the constantly changing nature of cybercrime limit their effectiveness. Overcoming these challenges requires a comprehensive strategy that emphasizes long-term policy reform, investments in infrastructure, culturally tailored awareness programs, and adaptive approaches to emerging cyber threats (Audu et al., 2023; UNESCO, 2022).

Theoretical Framework

This study was anchored on Social Learning Theory. Social Learning Theory was introduced by Albert Bandura during the 1960s, with its most notable exposition appearing in his 1977 book "*Social Learning Theory*". The framework highlights that individuals acquire behaviors, values, and skills by watching others, imitating their actions, and through reinforcement within social environments.

Social Learning Theory is grounded in the belief that learning is not limited to personal experience but also develops through observation and social engagement. The theory emphasizes that individuals can adopt new attitudes, behaviors, and skills by watching others and reflecting on the consequences of their actions. In this sense, observation becomes a crucial mechanism that influences how people think, behave, and respond across different contexts (Bandura, 1977).

One of the major components of the theory is observational learning, which explains that individuals often imitate the actions of family members, peers, or even role models in the media. This learning process is shaped by four conditions: paying attention to the behavior, retaining the information, having the ability to replicate it, and being motivated to do so. Without these elements, observation may not translate into actual behavior (Bandura, 1986).

Equally important is the idea of reciprocal determinism, which highlights the interaction between personal factors, environmental conditions, and behavior. Rather than being passive receivers of external influences, individuals actively engage with their surroundings, shaping and being shaped by them in return (Schunk, 2012).

The theory also emphasizes the role of reinforcement and punishment. While direct consequences guide behavior, people also learn indirectly by witnessing the rewards or penalties given to others. For example, watching someone benefit from secure online behavior may encourage imitation, whereas observing penalties for unsafe digital practices may discourage similar actions (Grusec, 1992).

Overall, Social Learning Theory positions learning as a social and interactive process rooted in observation, modeling, and feedback. It bridges the gap between behaviorist and cognitive perspectives, showing that human behavior evolves from a combination of external influences and internal cognitive processes.

The application of Social Learning Theory to the fight against cybercrime in Nigeria demonstrates how people gain knowledge and adopt safe digital practices by observing, imitating, and reinforcing the actions of others. Rather than relying solely on personal experiences, individuals learn by watching how others behave online and interpreting the outcomes of those behaviors (Bandura, 1977). For instance, when citizens observe friends, colleagues, or public figures practicing secure online habits, such as creating strong passwords, avoiding suspicious websites, or reporting fraudulent emails, they are more inclined to replicate those same behaviors.

Within this framework, public awareness campaigns play a central role. Initiatives that use media advertisements, workshops, or social media platforms to showcase proper cybersecurity practices provide visible examples for people to follow. These messages are more effective when they illustrate both the benefits of secure practices, such as protecting personal finances, and the risks of unsafe habits, like losing money through online fraud (Bandura, 1986).

Social Learning Theory also clarifies how digital literacy spreads through communities. Once an individual gains cybersecurity knowledge, they often share it within their social networks, creating a ripple effect. For example, a university student trained to identify phishing schemes may pass this knowledge to classmates, relatives, or neighbors, thereby strengthening the community's overall resilience. This process reflects Bandura's idea of reciprocal determinism, where individuals, their environment, and their actions continuously influence one another in shaping safe digital behaviors (Schunk, 2012).

Another important element of the theory is motivation. While awareness programs and training provide essential information, people are more likely to apply what they learn when they observe others being rewarded for safe online behaviors or punished for risky ones. For example, business owners who succeed by adopting secure e-commerce practices can serve as role models for others, while high-profile arrests and prosecutions of cybercriminals may discourage potential offenders from engaging in fraudulent activities (Grusec, 1992).

Thus, Social Learning Theory provides a valuable perspective for understanding how public awareness and digital literacy can be mobilized to prevent cybercrime in Nigeria. By emphasizing observation, imitation, reinforcement, and social interaction, the theory demonstrates that meaningful and lasting change requires not only individual learning but also collective influence within the broader social environment.

Empirical Review

Researchers and policymakers worldwide have increasingly focused on how best to prevent cybercrime and empower individuals to safeguard themselves in the digital space. A central consensus is that prevention strategies cannot rely exclusively on technological solutions or law enforcement responses; they must also consider human behavior, awareness, and digital skills. International evidence underscores that digital literacy and awareness play a vital role in reducing people's exposure to threats such as phishing, identity theft, and social engineering. For example, Kurniawan et al. (2022), through a systematic review, reported that individuals with stronger digital literacy are more capable of recognizing harmful online activities. However, they also cautioned that knowledge on its own does not guarantee safe behavior, as many users still take risks out of convenience or a low perception of danger. This underscores the need for ongoing reinforcement and practical forms of training.

Within Nigeria, research reveals that while awareness of cybercrime is widespread, protective behaviors are not consistently practiced. Hassan, Ajah, and Okpa (2025) found that although many Nigerians, particularly young people, are familiar with common online scams like phishing and fraud, there are still misunderstandings about how these threats operate and how to effectively guard against them. Broader African studies also suggest that socio-economic conditions, including unemployment and peer influence, intersect with online habits, shaping both vulnerability to cybercrime and, in some cases, participation in it. Thus, awareness by itself is not enough unless it is reinforced by broader social and institutional support.

Awareness campaigns have been widely explored as a tool for prevention. On the global stage, social media-based campaigns have proven effective for quickly reaching large groups and boosting short-term awareness. Yet, Bada and Sasse (2023) caution that long-term impact depends heavily on campaign design, with interactive and tailored approaches showing greater success than one-size-fits-all messages. In organizational settings, blending awareness training with hands-on exercises has been particularly impactful. Schops et al. (2024), for instance, showed through a field experiment that employees exposed to repeated phishing simulations coupled with feedback were less likely to fall victim than those who only received information. These findings highlight the importance of practical engagement and reinforcement in awareness initiatives.

Studies in Nigeria mirror these global insights but point out key structural challenges. Nwankwo et al. (2024) discovered that while Nigerian university students demonstrated higher awareness after digital safety workshops, many still engaged in unsafe habits, such as reusing passwords. This suggests that awareness efforts must be backed by institutional frameworks that promote and support secure practices. Although Nigeria's Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 offers a legal foundation for addressing cybercrime, its impact is limited by weak enforcement, inadequate forensic capacity, and delays in prosecution (Okunola & Adeniran, 2021). These systemic weaknesses reduce the overall effectiveness of preventive strategies.

Beyond the level of individual behavior, reviews have stressed the importance of linking awareness and digital literacy efforts to broader policy and community initiatives. Cenerva (2025) argues that in Nigeria, awareness programs need to be combined with investments in infrastructure, collaboration across agencies, and stronger enforcement to deliver meaningful results. Evidence from other contexts shows that integrating education with institutional reforms produces the most lasting outcomes. For instance, Granito et al. (2025) found that organizations combining awareness training with policy changes achieved stronger cybersecurity performance compared to those that implemented either strategy in isolation.

Therefore, existing evidence suggests that while legal and technological tools are essential for cybercrime prevention, people-centered strategies, such as digital literacy programs and continuous awareness campaigns, are equally crucial. To be effective, these efforts must be practical, long-term, and supported by both institutional mechanisms and socio-economic reforms. For Nigeria, this translates into scaling up awareness education in schools and workplaces, strengthening enforcement of existing laws, and tackling the social factors that heighten cyber risks. Globally, the research emphasizes the value of integrated approaches that combine education, practice, and policy for sustainable cybercrime prevention.

Methodology

This research employed a qualitative design, as it seeks to gain a deeper understanding of issues related to cybercrime prevention, public awareness initiatives, and digital literacy. A qualitative approach is most suitable because it emphasizes context, interpretation, and meaning rather than statistical generalizations. It enables the researcher to examine how previous studies, policies, and interventions have addressed cybercrime, while also assessing their outcomes in Nigeria and internationally. By doing so, the study provides a comprehensive narrative that brings out recurring trends, gaps, and lessons from academic and institutional sources.

For data collection, the study makes use of secondary sources, which include scholarly journal articles, textbooks, government publications, policy documents, and reputable online materials on cybercrime, awareness campaigns, and digital literacy. The use of secondary data is justified as it offers access to a broad pool of existing empirical evidence and theoretical viewpoints already established by researchers and practitioners. It also allows the investigation to cover both local (Nigerian) and global contexts without the practical limitations associated with primary data collection. The materials were carefully selected based on their relevance, reliability, and recency, with particular emphasis on peer-reviewed studies and official reports.

The data were analyzed using thematic analysis, a method that helps identify, group, and interpret recurring themes across qualitative information. After reviewing the selected literature, the findings were organized into key thematic areas such as: (a) the effectiveness of awareness campaigns, (b) the role of digital literacy in curbing cybercrime, (c) institutional and policy-related challenges, and (d) strategies considered best practices in prevention. Thematic analysis was considered appropriate because it offers a structured yet flexible framework for examining qualitative data, making it possible to draw meaningful insights and well-grounded conclusions.

Conclusion and Recommendations

Cybercrime remains a major obstacle to Nigeria’s economic progress, social stability, and international image. While the spread of internet connectivity and mobile technologies has brought about innovation and growth, it has equally opened doors to new forms of digital threats targeting individuals, organizations, and state institutions. Although legal instruments such as the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 exist, and security agencies continue their efforts, the continued rise of offenses like phishing, identity theft, and financial scams illustrates the shortcomings of legal responses when they are not reinforced by broader preventive measures.

This study shows that tackling cybercrime in Nigeria requires more than enforcement and punitive approaches. True resilience lies in equipping citizens with the knowledge to detect risks and the skills to safeguard themselves online. Public awareness plays a key role in helping people recognize suspicious activities, while digital literacy enables them to take concrete protective steps such as creating strong passwords, spotting phishing schemes, and adopting secure online platforms. Evidence from Nigeria and other parts of the world demonstrates that countries that invest in digital literacy and awareness achieve greater protection against cybercrime and build stronger trust in digital systems.

Nevertheless, issues of inclusivity and sustainability persist. In Nigeria, most awareness efforts are concentrated in urban areas, leaving rural communities less informed and more vulnerable. In addition, weak institutional capacity, poor collaboration between stakeholders, and socio-economic pressures continue to hinder progress. This highlights the need for a holistic strategy, one that integrates legislation, technological safeguards, awareness initiatives, and literacy programs, while also fostering community participation and institutional strengthening.

In conclusion, Nigeria’s fight against cybercrime cannot be won by legal frameworks alone. A people-focused strategy that emphasizes education, awareness, and community engagement is vital to complement existing measures. By strengthening digital education, broadening the scope of awareness campaigns, building effective partnerships, and empowering communities, Nigeria can foster a culture of digital resilience. Such an approach would not only curb cybercrime but also enhance public confidence in the digital economy, thereby supporting national security, economic growth, and the nation’s global reputation. To strengthen Nigeria’s response to cybercrime and build a more resilient digital society, the following recommendations are proposed:

i. The Nigerian government should embed digital literacy into school curricula from primary to tertiary levels. Beyond basic ICT, students should learn cybersecurity essentials such as safe browsing, password protection, and online privacy. Teaching these skills early will prepare young people to engage safely and confidently in the digital world.

ii. Awareness campaigns should be expanded to rural and semi-urban areas, using local languages and culturally relevant messages. Platforms like community radio, religious gatherings, and grassroots organizations can improve outreach. This ensures vulnerable groups gain the knowledge to reduce exposure to cyber risks.

iii. The government should strengthen public-private partnerships to sustain cybersecurity education. Collaboration with telecoms, banks, tech firms, and civil society will provide funding and expertise. Such partnerships also ensure training programs remain current with evolving digital threats and global best practices.

iv. Organizations should provide continuous cybersecurity training for employees instead of one-time programs. Regular workshops, phishing simulations, and refresher courses will help workers recognize emerging risks. These efforts not only safeguard personal data but also protect organizational assets from cyber threats.

v. The Nigerian government should support community-based awareness initiatives through trusted local actors such as youth groups, religious leaders, and influencers. Their involvement makes campaigns relatable and credible at the grassroots level. This approach fosters collective responsibility, treating cybersecurity as a shared social duty.

References

Ajayi, E. F. G. (2021). Routine Activity Theory and cybercrime victimization in Nigeria. International Journal of Cyber Criminology, 15(2), 145–162.

Audu, J., Nwogu, A., & Afolabi, O. (2023a). Cybercrime and the challenges of cybersecurity in Nigeria: Policy and societal implications. Journal of African Security Studies, 32(2), 145–160. https://doi.org/10.1080/xxxxxx

Audu, J., Nwogu, A., & Afolabi, O. (2023b). Cybercrime trends in Nigeria: Emerging threats and policy responses. Journal of African Digital Studies, 5(1), 34–49.

Bada, A., & Sasse, A. M. (2023). A systematic review of current cybersecurity training methods. Safety Science, 168, 106965. https://doi.org/10.1016/j.ssci.2023.106965

Bandura, A. (1977). Social learning theory. Englewood Cliffs, NJ: Prentice Hall.

Bandura, A. (1986). Social foundations of thought and action: A social cognitive theory. Englewood Cliffs, NJ: Prentice-Hall.

Cenerva. (2025). Strengthening Nigeria's response to cybercrime. Policy Report. Retrieved from https://cenerva.com

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588–608.

Eze, S. C., & Eze, E. (2021). Digital literacy and cybersecurity awareness as strategies for combating cybercrime in Nigeria. Journal of Information and Communication Technology, 20(3), 67–81.

Eze, V., & Eze, C. (2021). Digital literacy and cybersecurity awareness in Nigeria: Challenges and opportunities. African Journal of Information Systems, 13(2), 77–90.

Granito, M., Oaklands, L., & Chen, H. (2025). Understanding the efficacy of phishing training in practice: A randomized field experiment. Journal of Cybersecurity Education, Research and Practice, 8(2), 44–61.

Grusec, J. E. (1992). Social learning theory and developmental psychology: The legacies of Robert Sears and Albert Bandura. Developmental Psychology, 28(5), 776–786. https://doi.org/10.1037/0012-1649.28.5.776

Hassan, I. M., Ajah, B. O., & Okpa, J. T. (2025). Emerging trends in cybercrime awareness in Nigeria. International Journal of Cybersecurity Studies, 4(1), 23–35.

Igbinedion, J., & Aladenusi, T. (2022). Cybersecurity campaigns in Nigeria: An evaluation of strategies and effectiveness. Nigerian Journal of Policy and Strategy, 9(3), 201–219.

Kurniawan, S., Al-Mamun, M. A., & Widodo, H. (2022). A systematic review on digital literacy. Smart Learning Environments, 9(23), 1–17. https://doi.org/10.1186/s40561-022-00187-7

Ndukwe, O., & Okoli, C. (2022). The growth of cybercrime and the need for cyber hygiene in Nigeria. Nigerian Journal of Criminology and Security Studies, 8(2), 89–104.

Nwankwo, F. C., Obinna, C. J., & Eze, J. I. (2024). Cybersecurity awareness of university students in Nigeria: Analysis and implications. African Journal of Information Systems, 16(3), 55–72.

Obi, P., & Osho, G. (2023a). Cybercrime, digital literacy and Nigeria's digital future: An assessment of youth vulnerabilities. International Journal of Cyber Policy, 8(4), 211–229.

Obi, P., & Osho, G. (2023b). Cybersecurity awareness and victimization among Nigerian internet users. Journal of African Studies and Security, 8(2), 55–72.

Okeshola, F., & Adeta, A. (2022). Cybercrime and national security in Nigeria: An assessment. Journal of Contemporary Security Studies, 6(4), 66–84.

Okunola, A. O., & Adeniran, A. I. (2021). Cybercrime and cyber law in Nigeria: Challenges and way forward. Journal of Law and Judicial System, 12(2), 15–29.

Schops, D., Lin, T., & Mayer, R. (2024). Simulated phishing campaigns as a tool for behavioural change: A field experiment in cybersecurity. USENIX Security Symposium Proceedings, 33(1), 233–247.

Schunk, D. H. (2012). Learning theories: An educational perspective (6th ed.). Boston, MA: Pearson Higher Education.

UNESCO. (2022). Digital literacy for life and work. United Nations Educational, Scientific and Cultural Organization. Retrieved frm https://unesdoc.unesco.org on 25th June, 2025.