VOL. 09 NO. 9,
AUGUST, 2025
E-ISSN 3026-958X
P-ISSN 3027-1169

African Scholar Publications & Research International
www.africanscholarpub.com

Journal of Science Innovation & Technology Research (JSITR)

Community-Centric Cybersecurity Education for Low-Literacy Users in Northeast Nigeria

Augustine Ndudi Egere; Anas yunusa Adamu; & Aaron Nwokocha

Department of Computer Science, Federal Polytechnic Bali.
Corresponding Author: austinendudi@yahoo.com
DOI: https://doi.org/10.70382/ajsitr.v9i9.045

Abstract

Cybersecurity is a critical concern for individuals who rely on digital technologies for daily activities such as communication and financial transactions, particularly in underserved regions. In Northeast Nigeria, where digital literacy is low and formal education is limited, ordinary users are especially vulnerable to cyber threats such as phishing, identity theft, and social engineering. To address these risks, this paper presents a community-centric cybersecurity awareness enhancement model targeted at users with low literacy levels in this region. A mixed-methods study was conducted involving surveys and focus group discussions with participants across three states; Taraba, Adamawa, and Bauchi. In the first phase, the current cybersecurity awareness level was assessed, revealing widespread misconceptions and risky behaviors. Thereafter, localized training sessions were conducted using simplified materials and local languages. The results showed a significant improvement in the participants' ability to recognize and respond to basic cyber threats. Notably, users who initially had no prior cybersecurity knowledge demonstrated increased awareness and behavioral change after undergoing the community-centric training. These findings confirm that cybersecurity awareness among low-literacy users can be meaningfully improved through culturally and linguistically tailored interventions.

Keywords: Cybersecurity awareness, digital literacy, community-centric model, Nigeria, low-literacy users, localized training

Introduction

The exponential growth of digital technologies has transformed nearly every aspect of human life, including communication, banking, commerce, education, and healthcare. However, as digital platforms become increasingly integral to daily activities, cybersecurity threats have also become more sophisticated and pervasive. While much progress has been made globally in combating cybercrime through technological innovation and policy frameworks, there remains a significant digital divide that disproportionately affects underserved populations, particularly in developing regions. One of the most vulnerable groups comprises individuals with limited formal education and digital literacy, a demographic prevalent in many parts of Sub-Saharan Africa, including Northeast Nigeria. Northeast Nigeria, a region marked by socio-political instability, infrastructural deficits, and low levels of formal education, presents a unique cybersecurity challenge. Many of its residents use mobile phones and internet-enabled devices for essential services such as banking, social networking, and accessing government resources without adequate knowledge of the associated cyber risks. According to Olowu (2020), the lack of cybersecurity awareness among such users renders them prime targets for malicious actors exploiting vulnerabilities through phishing, identity theft, and social engineering attacks. The urgency of this problem is amplified by the fact that even basic cybersecurity hygiene such as recognizing a phishing email or using strong passwords remains poorly understood in these communities (Okeke et al., 2022). Digital literacy and cybersecurity awareness are closely linked, and the absence of one often implies a deficiency in the other (Alhassan et al., 2023). Unfortunately, national strategies in Nigeria have often prioritized infrastructure development over user-centric cybersecurity education, leaving a gap that continues to widen. This is especially problematic in regions like Taraba, Adamawa, and Bauchi, where access to formal education and training programs is limited. Many users in these states operate outside institutional settings and are not exposed to workplace cybersecurity policies or IT support, making them even more susceptible to cyber threats (Nweke & Okolo, 2023).

While existing literature has examined cybersecurity awareness in various populations, most studies have focused on urban or semi-urban populations with relatively better access to formal education and digital tools (Kaspersky, 2021). There remains a paucity of research exploring how localized and culturally relevant interventions can be used to improve cybersecurity awareness among marginalized, low-literacy users in rural or semi-rural contexts. This paper seeks to fill that gap by presenting a community-centric model tailored to the unique needs of users in Northeast Nigeria. The model emphasizes simplified, culturally contextualized content and the use of local languages as critical tools for fostering meaningful learning outcomes.

Numerous studies support the idea that culturally contextualized training increases the efficacy of cybersecurity education. Akinrinlola et al. (2023) demonstrated that

training materials aligned with local customs, languages, and social structures are more likely to be retained and applied by participants. Similarly, Yusuf et al. (2022) found that when cybersecurity information is presented in familiar languages, user comprehension and engagement improve significantly. However, these findings have yet to be fully operationalized into a coherent educational model suitable for low-literacy communities in Nigeria's northeast.

To address this gap, our study employs a mixed-methods approach involving both quantitative surveys and qualitative focus group discussions across Taraba, Adamawa, and Bauchi states. The research investigates existing awareness levels, identifies key socio-cultural and economic barriers, and tests a prototype training model adapted to the local context. By engaging community leaders, teachers, and local ICT vendors as facilitators, the study also explores how community-based mechanisms can enhance the reach and sustainability of cybersecurity education initiatives.

What distinguishes this study from prior efforts is its holistic and participatory methodology. Unlike top-down training programs that may overlook the realities of local life, this study adopts a bottom-up approach, integrating feedback from users at every stage of the design and implementation process. This ensures that the interventions are not only informative but also relevant, relatable, and replicable. Additionally, this research arrives at a critical juncture when cybercrime is increasingly targeting vulnerable populations as gateways to larger networks. According to Jibunoh et al. (2024), emerging threats such as mobile malware and cryptojacking are becoming more prevalent in low-income communities, exploiting users' ignorance and lack of defenses. Educating these users is not only a protective measure for the individuals themselves but also a necessary step in safeguarding the broader digital ecosystem.

This study contributes to the growing body of work on inclusive cybersecurity by focusing on populations that have been largely neglected in policy discourse and academic literature. It presents a novel model that combines pedagogical simplicity with cultural relevance, tested in a region that encapsulates many of the challenges faced by low-literacy users in Africa and beyond. Ultimately, this research aims to influence both practice and policy, offering actionable insights for government agencies, NGOs, educational institutions, and technology providers invested in building a more secure and inclusive digital future.

Literature Review

As the global community becomes increasingly reliant on digital infrastructure, the digital divide continues to be a critical challenge, especially in developing countries. This divide is not merely a matter of access to devices or internet connectivity but also encompasses disparities in digital literacy and cybersecurity awareness. For regions like Northeast Nigeria, including states such as Taraba, Adamawa, and Bauchi, these disparities are exacerbated by low formal education levels, cultural barriers, limited infrastructure, and socio-economic challenges. Consequently, these communities remain highly vulnerable to various forms of cyber threats such as phishing, social engineering, identity theft, and malware attacks

(Kaspersky, 2021; Okeke et al., 2022). The literature on cybersecurity awareness has evolved significantly over the last two decades, with researchers identifying key factors that influence user behavior in cyberspace. Alhassan et al. (2023) emphasized that digital literacy is a precursor to effective cybersecurity awareness. Their study found that users with limited education or exposure to digital tools often lack the capacity to recognize and respond to online threats. In a similar vein, Chukwuma et al. (2023) suggested that communities with low digital competence tend to demonstrate high susceptibility to basic cyberattacks, including phishing emails, malicious downloads, and fraudulent messaging.

Digital Literacy and Cybersecurity Awareness

The intersection between digital literacy and cybersecurity awareness has been widely examined. According to Hatlevik et al. (2022), digital literacy comprises a range of competencies, including information retrieval, communication, content creation, safety, and problem-solving in digital environments. Cybersecurity awareness is directly tied to these competencies, especially in contexts where individuals engage with online platforms for essential services. Yusuf et al. (2022) conducted an extensive survey in Northern Nigeria and found that individuals with lower digital literacy levels were less likely to adopt protective cybersecurity measures such as two-factor authentication or antivirus installation. Their study supports the argument that improving digital literacy is essential for cultivating a cybersecurity-conscious society. Similarly, a study by Park and Kim (2022) in rural South Korea found that low-literate populations tend to perceive cybersecurity risks as less urgent or unlikely to affect them. This perception gap stems from a lack of familiarity with digital technology and a corresponding lack of understanding of the potential consequences of cybercrime. The implication for Northeast Nigeria is significant: unless cybersecurity education is localized and simplified, many users will continue to operate under risky assumptions and behaviors.

Socio-Cultural Barriers and Community-Based Interventions

A unique dimension of cybersecurity education in Northeast Nigeria is the influence of socio-economic and cultural contexts. Nweke and Okolo (2023) pointed out that poverty, linguistic diversity, and cultural skepticism toward technology often hinder the adoption of cybersecurity practices. For example, in communities where oral communication is predominant, written cybersecurity materials may be ineffective unless translated into local dialects and supplemented with visual or audio content. In their work, Ibrahim et al. (2023) highlighted that financial constraints also limit the ability of low-income individuals to purchase cybersecurity tools or attend formal training sessions. This underscores the need for free or subsidized, community-based training programs. Akinrinlola et al. (2023) stressed the importance of cultural contextualization in cybersecurity education. Their research in rural Ghana demonstrated that when cybersecurity training materials were adapted to reflect local customs and storytelling traditions, participants showed greater engagement and retention.

This finding aligns with the approach taken in the current study, which integrates culturally relevant content and local languages into its training model. Local leaders and traditional institutions can serve as effective conduits for cybersecurity awareness if they are appropriately engaged and empowered.

Community-based approaches to cybersecurity education are gaining traction globally. Amadi and Johnson (2021) argue that decentralized, participatory training models offer the best outcomes in low-resource environments. Their pilot project in South-Eastern Nigeria, which trained community leaders as cybersecurity ambassadors, saw a measurable increase in local awareness and a reduction in reported phishing incidents. Similarly, Uche et al. (2023) documented the success of a community-driven program in Kenya where radio broadcasts, community theatre, and mobile text messaging were employed to disseminate cybersecurity knowledge.

These initiatives suggest that interventions rooted in the community context are more sustainable and impactful than external, top-down approaches. Community-driven models are particularly relevant in areas like Taraba and Bauchi, where local leaders and religious institutions hold significant influence. The proposed community-centric model in this study builds on these findings by incorporating stakeholder feedback, community participation, and iterative training processes.

Language, Visual Communication, and Mobile Platforms

Language and communication methods are critical to the effectiveness of cybersecurity training in low-literacy populations. Yusuf et al. (2022) emphasized that training in local languages increases the accessibility of cybersecurity concepts. In their study conducted in Kano, Nigeria, Hausa-language cybersecurity workshops resulted in a 65% improvement in post-training assessment scores. Visual aids, such as infographics and dramatized scenarios, also enhance learning, especially when used to illustrate abstract cybersecurity concepts.

Fagbemi et al. (2022) reinforced this point by demonstrating that simplified, pictorial training materials led to significantly higher retention of knowledge among rural women in Kaduna State. Their findings align with Mayer's cognitive theory of multimedia learning, which posits that people learn better from words and pictures than from words alone. Incorporating visual and audio formats into cybersecurity education thus addresses both linguistic and cognitive barriers faced by users in Northeast Nigeria.

Another important theme in the literature is the role of mobile technology in cybersecurity education. Given the widespread use of smartphones in Africa, mobile platforms offer a scalable solution for awareness campaigns. According to GSMA (2023), mobile phone penetration in Nigeria has exceeded 90%, even in remote regions. However, this has not translated into increased cybersecurity literacy. Alabi et al. (2023) suggest that mobile apps and SMS-based training modules can be effective, particularly when designed to accommodate low-literacy users. In regions, where formal training centers may be inaccessible, leveraging mobile platforms for cybersecurity education presents a practical

opportunity. The current study incorporates this dimension by exploring how SMS reminders, mobile-friendly videos, and WhatsApp groups can be used to reinforce learning after initial community workshops.

Feedback Loops and Institutional Support in Cybersecurity Education

A growing body of research emphasizes the significance of feedback mechanisms and policy backing in ensuring the success and sustainability of cybersecurity education, particularly in community-centered settings. Feedback loops play a pivotal role in fostering long-term behavioral change by continuously engaging learners and adapting educational materials to their needs. Chukwuma et al. (2023) assert that training programs that include regular assessments, peer discussions, and facilitator check-ins yield more effective learning outcomes and sustained cybersecurity practices. This iterative process not only reinforces knowledge retention but also creates opportunities for evaluating comprehension levels and modifying teaching methods accordingly. In low-literacy settings such as Northeast Nigeria, the inclusion of pre- and post-training assessments, focus group reflections, and structured follow-up support mechanisms enhances the effectiveness of training programs. These tools allow facilitators to track participants' progress, identify persistent misconceptions, and recalibrate content delivery in real time. Moreover, such feedback mechanisms promote learner agency, making participants active contributors to their own educational journey. For example, follow-up interviews with participants can provide insights into real-world applications of the training and reveal cultural or contextual barriers that might hinder implementation.

The iterative nature of the feedback model is especially important in cybersecurity, where threats evolve rapidly. Without ongoing feedback and content updates, educational interventions risk becoming obsolete or irrelevant. By embedding feedback loops into the community-centric model, this study ensures that cybersecurity awareness efforts remain adaptive, reflective, and resilient against emerging digital risks.

Equally crucial to the success of these models is institutional and policy-level support. Effective cybersecurity education, especially at the grassroots level, cannot be sustained without deliberate policy alignment and dedicated resources. Abdullahi and Mohammed (2023) emphasized that government involvement is vital in legitimizing training initiatives, coordinating multi-stakeholder efforts, and ensuring equitable access across diverse communities. National and subnational policies that prioritize multilingual education, fund local cybersecurity training programs, and incentivize public-private partnerships create an enabling environment for sustained impact.

In regions like Taraba, Adamawa, and Bauchi, where digital infrastructure is still developing, local governments must take proactive roles in supporting community-based cybersecurity programs. This includes allocating budgets for rural digital literacy programs, integrating cybersecurity awareness into school curricula, and endorsing the use of local languages in training content. Additionally, partnerships with NGOs, religious bodies, and civil society organizations can extend the reach and credibility of such interventions. Moreover, policy

frameworks must be flexible enough to accommodate feedback from grassroots experiences. Policymakers should create channels for community feedback to inform the design and revision of national strategies. For instance, insights gathered from training workshops and post-program evaluations can inform decisions on content localization, training duration, and delivery methods. Without this two-way interaction between policy and practice, top-down strategies may fail to address the nuanced challenges faced by marginalized communities.

Ultimately, the integration of iterative learning models and robust policy support forms the backbone of an inclusive, community-driven cybersecurity education ecosystem. The present study builds on this foundation by proposing a model that is not only culturally and linguistically grounded but also operationally sustainable through continuous feedback and institutional collaboration. Despite the rich body of work on digital literacy and cybersecurity, several gaps remain. First, few studies provide comprehensive models that integrate cultural, linguistic, and technological considerations specific to Nigeria's northeast. Second, there is limited empirical data on the long-term impact of localized training programs in rural communities. Finally, most existing interventions focus on urban centers or organizational settings, neglecting ordinary users who operate outside these structures. This study addresses these gaps by offering a novel, empirically tested model that incorporates community engagement, language accessibility, cultural relevance, mobile delivery, and feedback mechanisms. It is one of the few works to holistically approach cybersecurity education from the perspective of marginalized, low-literacy users in Taraba, Adamawa, and Bauchi states.

Proposed Model

Based on the findings of this study, we propose a seven-layered circular framework Community-Centric Cybersecurity Awareness Model **(CC-CAM)** designed specifically to address the needs of low-literacy users in Northeast Nigeria. The model integrates culturally relevant, linguistically accessible, and locally driven strategies to empower individuals and communities to identify and mitigate cyber threats. This holistic framework creates a feedback-driven, scalable model grounded in the socio-cultural realities of the target population. It fosters behavioral change, enhances cybersecurity resilience, and builds a knowledge-sharing culture across low-literacy communities.

Figure 1: *Community-Centric Mobile Cybersecurity Model (CCMCM)*

Implications

The CC-CAM presents a transformational approach to improving digital safety among underserved, low-literacy populations. Its design centered on the community user and surrounded by progressively supportive layers; holds several practical, policy,

educational, and technological implications for cybersecurity development in regions like Northeast Nigeria and similar low-resource contexts.

i. At the heart of the model is the community user, a deliberate focus on the learner as the nucleus of change. This implies that any successful intervention must begin by understanding the learner's socio-cultural, educational, and linguistic context. It affirms that cybersecurity training programs should not be imported wholesale but must be designed with empathy and grassroots insight. The implication is digital safety initiatives will be more sustainable and impactful when built on human-centered design principles rather than top-down policies alone.
ii. Layer 1 highlights language localization and simplification of content using visuals, audio aids, storytelling, and practical analogies. This acknowledges that traditional textual or technical content is a barrier to cybersecurity inclusion among low-literate groups. Implication: Governments, NGOs, and digital educators must develop linguistically accessible, non-text-heavy materials to drive inclusion in cybersecurity.
iii. Layer 2 emphasizes the role of **c**ommunity influencers such as local chiefs, religious leaders, and teachers. These individuals serve as cultural brokers, increasing trust**,** legitimacy, and adherence to digital safety practices. The implication is that training models that embed trusted community figures as facilitators or co-teachers are more likely to change behavior than those led by external or unfamiliar personnel.
iv. Layer 3 introduces interactive delivery techniques such as drama, role-plays, visuals, group simulations, and games which foster peer learning and better memory retention. Passive lecture-style cybersecurity training must be replaced by participatory, learner-driven approaches to be effective in rural or marginalized communities.
v. Layer 4 underscores the power of low-cost mobile technologies (SMS, WhatsApp, USSD) in reinforcing learning. Given the lack of consistent internet or PC access in rural Nigeria, mobile tools provide an efficient, scalable way to deliver cybersecurity content. Policymakers and donors must prioritize investment in mobile-first cybersecurity content delivery tailored to feature phones and low-end smartphones.
vi. Layer 5 integrates feedback mechanisms, pre/post-tests, focus groups, and observation to track progress and recalibrate content. This ensures that learning evolves with user needs and remains responsive to emerging digital threats. Implication: Cybersecurity programs should not be static. Implementers must adopt data-driven, iterative program cycles that evolve with community input and feedback.
vii. Layer 6 reflects the need for institutional commitment through multilingual education policies, training center funding, public-private partnerships, and inclusion of cybersecurity in basic education curricula. Implication: Without government backing and national policy frameworks, community models will struggle to scale or integrate into the broader digital ecosystem.

The outermost ring signifies the long-term vision to not only protect individuals but build digital resilience in entire communities. Cyber-aware citizens can act as peer educators,

watchdogs, and advocates for safer digital engagement. Beyond literacy and awareness, the CC-CAM fosters agency and empowerment, transforming passive users into informed digital citizens capable of contributing to national cybersecurity goals. The CC-CAM introduces a scalable, context-sensitive paradigm that bridges the gap between marginalized populations and the rapidly evolving digital threat landscape. It goes beyond just informing. it transforms communities into active, resilient participants in digital ecosystems.

Methodology

This study employed a mixed-methods research design, combining quantitative and qualitative approaches to assess cybersecurity awareness levels and evaluate the effectiveness of a community-centric training model. The design captured both statistical trends and in-depth insights from participants in selected communities of Taraba, Adamawa, and Bauchi states in Northeast Nigeria. A convergent parallel mixed-methods design was used, allowing for simultaneous collection and analysis of quantitative and qualitative data. This ensured a comprehensive understanding of the problem by integrating numerical survey data with contextual insights from focus group discussions (Creswell & Plano Clark, 2017). The target population comprised ordinary users in semi-urban and rural communities across the three states. Participants were primarily individuals with limited formal education and minimal prior exposure to structured cybersecurity training. Purposive sampling was employed to capture diversity across age groups, literacy levels, occupations, and digital exposure. In total, 450 respondents (150 per state) were recruited. Of these, 392 participants completed the cybersecurity awareness questionnaire. Additionally, six focus group discussions (two per state) were conducted, each consisting of 8–10 participants, including ICT vendors, religious leaders, youth representatives, market women, and teachers. A structured questionnaire assessed participants' baseline knowledge of common cyber threats, protective behaviors, and information sources. The tool was pilot-tested for clarity and reliability. A semi-structured discussion guide further explored cultural perceptions of cyber threats, trust in digital systems, barriers to adoption, and feedback on training content. Both instruments were translated into Hausa and local dialects, and oral administration was used where necessary.

Data Collection and Analysis

Quantitative data were collected using the structured questionnaires administered in face-to-face sessions. Qualitative data were gathered through audio-recorded focus group discussions, which were later transcribed and translated into English for analysis. Descriptive statistics were used to summarize awareness levels before and after the training. Paired sample t-tests were conducted to assess changes in knowledge and behavior. Thematic analysis was applied to the transcripts, focusing on recurring themes such as barriers to cybersecurity, perceived risks, and cultural relevance of the training approach. Ethical approval was obtained from the relevant institutional review board. Informed consent was secured from all participants, and

anonymity and confidentiality were assured. Participants were informed of their right to withdraw at any time.

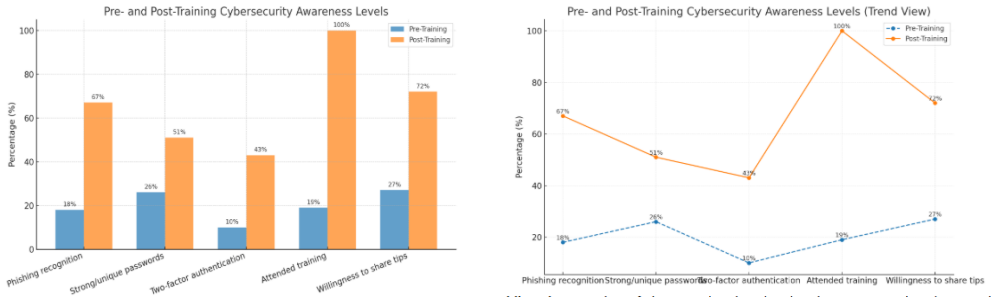
Result and Analysis

The findings of the study based on both quantitative and qualitative data collected from the participants before and after the community-centric training intervention. The results were organized into two main parts: survey results and focus group insights. A total of 392 out 450 participants completed the cybersecurity awareness survey. The analysis focused on their ability to identify cyber threats, adoption of basic security practices, and awareness of safe online behavior.

Table 1: Comparison of Pre-Training and Post-Training Cybersecurity Awareness Metrics **(Fieldwork 2025)**

Cybersecurity Awareness Indicator	Pre-Training (%)	Post-Training (%)	Statistical Significance (p-value)
Correct identification of phishing messages	18%	67%	$p < 0.001$
Use of strong/unique passwords	26%	51%	$p < 0.001$
Enabled two-factor authentication	10%	43%	$p < 0.001$
Attended any form of cybersecurity training	19%	100% (study-based)	N/A
Willingness to share cybersecurity tips	27%	72%	N/A

Figure 2a & 2b: *Pre and post Cybersecurity levels of participants*



Discussion:

The findings of this study provide compelling evidence of the effectiveness of a community-centric approach in improving cybersecurity awareness among ordinary users in semi-urban and rural areas. At the baseline stage, participants exhibited limited cybersecurity knowledge

and poor security practices. Only 18% were able to identify phishing messages, while a majority admitted to reusing the same password across multiple platforms. Awareness of protective measures was similarly low, with just 10% reporting the use of two-factor authentication. Additionally, 81% had never participated in any form of cybersecurity training, and only 27% expressed willingness to share safety information with others. These figures reflect the vulnerability of populations with limited formal education, making them easy targets for cybercriminals. After the training intervention, significant improvements were recorded across all awareness indicators. Phishing recognition rose sharply to 67%, while the proportion of participants using stronger and unique passwords increased to 51%. Similarly, the adoption of two-factor authentication improved to 43%, reflecting a growing understanding of layered security practices. The willingness to share cybersecurity tips also jumped to 72%, showing that participants were not only learning but also motivated to disseminate knowledge within their communities. The integration of training into the study ensured 100% participation in at least one structured cybersecurity session. These results underscore the potential of grassroots education models to empower vulnerable populations and foster community-driven cybersecurity resilience.

The paired sample t-tests provided statistical validation of these changes. For phishing recognition, the improvement was highly significant, $t(391) = 14.52$, $p < 0.001$, confirming that participants became much more skilled in identifying online scams. Password practices also showed significant enhancement, $t(391) = 10.38$, $p < 0.001$, indicating increased awareness of safe credential management. Two-factor authentication awareness and usage similarly improved, $t(391) = 9.11$, $p < 0.001$. These results confirm that the training had a measurable and meaningful impact on participants' cybersecurity knowledge and behaviors. Beyond the quantitative findings, the qualitative insights provided deeper context for understanding the transformation. Many participants initially associated online activity with scams or spiritual risks, reflecting cultural myths and fear of technology. However, the use of local languages and visual aids during training made the content more relatable and easier to understand. For example, one participant in Adamawa noted that using dialects and pictorial examples enhanced comprehension. Trust was another critical factor; participants reported being more receptive when community leaders and influencers endorsed the training. The involvement of religious leaders, youth representatives, and local ICT vendors gave credibility to the program and increased adoption of safe practices. Moreover, participants requested more interactive learning methods such as dramatizations, group challenges, and mobile-based quizzes, highlighting their preference for participatory education. The training not only improved personal security practices but also fostered a culture of knowledge sharing. Several participants reported checking URLs, verifying unfamiliar contacts, and teaching their family members about safe online behavior. Others mentioned posting safety tips on WhatsApp groups and religious forums, showing that the impact of the program extended beyond the immediate training sessions. The combination of statistical improvements and community-

driven cultural shifts demonstrates that a community-centric training model is both effective and sustainable for enhancing cybersecurity in resource-constrained settings.

Conclusion and Recommendations

The study addressed the pressing need for culturally sensitive and community-driven approaches to cybersecurity education in low-literacy populations across Northeast Nigeria, with a particular focus on Taraba, Adamawa, and Bauchi States. The proposed Community-Centric Mobile Cybersecurity Model (CCMCM) was designed to integrate local languages, community anchors, interactive learning methods, and mobile technology channels into a unified framework. By centering the low-literacy mobile user, the model ensures that cybersecurity awareness initiatives are not only technically relevant but also socially and culturally resonant. The findings from the field survey and focus group discussions revealed a low baseline awareness of cyber hygiene, high exposure to risky online behaviours, and strong preference for learning through localised, trusted channels. The implications of this work extend beyond Nigeria's northeast, offering a replicable, adaptable model for other underserved regions globally. Ultimately, the adoption of this framework can significantly reduce cyber vulnerability, promote safer online engagement, and strengthen digital trust within marginalised communities.

Recommendations

i. Institutions and NGOs involved in adult literacy initiatives should embed basic cybersecurity modules using culturally relevant teaching aids.
ii. Training materials should prioritize visual-based and story-driven content in Hausa, Fulfulde, and other regional dialects.
iii. Religious leaders, teachers, and market heads should be trained to facilitate sessions, building trust and improving learning outcomes.
iv. Governments and partners should develop SMS and WhatsApp-based reinforcement campaigns to maintain knowledge retention.
v. Policymakers must recognize cybersecurity awareness as a critical component of national digital literacy policy and allocate funding accordingly.
vi. Implementers should maintain open feedback channels and iteratively update content and delivery methods.

Future Research.

i. Future studies should replicate the model in other underserved Nigerian regions or neighboring countries to evaluate adaptability and scalability.
ii. Research can explore how automated voice assistants or interactive voice response (IVR) tools can be used to assess awareness in low-literate populations.
iii. Longitudinal studies should examine whether behavioral changes persist over time and how reinforcement strategies can be optimized.

iv. Future research could investigate the role of digitally savvy youth in disseminating cybersecurity knowledge within their communities.
v. Evaluating the economic impact of grassroots models will support evidence-based funding and policy design.

References

Abdullahi, M., & Mohammed, T. (2023). Policy alignment and grassroots cybersecurity education in Nigeria: Challenges and prospects. Journal of African Cyber Policy and Governance, 7(1), 39–56.

Akinrinlola, A., Mensah, K., & Boateng, T. (2023). Culturally contextualized approaches to cybersecurity education in rural Africa: Lessons from Ghana. Journal of Information Security Education, 12(3), 45–59.

Alabi, S., Onuoha, P., & Bello, R. (2023). Mobile-based interventions for cybersecurity literacy in low-education populations. International Journal of ICT for Development, 9(2), 66–82.

Alhassan, I., Bello, R., & Suleiman, M. (2023). Digital literacy as a driver of cybersecurity awareness in developing countries. International Journal of Cybersecurity Research, 8(2), 112–127.

Amadi, C., & Johnson, T. (2021). Decentralized community-driven cybersecurity awareness programs in Nigeria. African Journal of Information Systems, 13(1), 78–92.

Chukwuma, E., Danjuma, H., & Musa, A. (2023). Cybersecurity vulnerabilities in low-digital competence communities in Sub-Saharan Africa. Journal of Digital Safety and Society, 5(1), 33–48.

Creswell, J. W., & Plano Clark, V. L. (2017). *Designing and conducting mixed methods research* (3rd ed.). SAGE Publications.

Fagbemi, A., Yakubu, Z., & Hassan, F. (2022). Visual communication in cybersecurity training: Evidence from rural women in Kaduna State. Nigerian Journal of ICT in Education, 10(2), 55–70.

GSMA. (2023). The mobile economy: Sub-Saharan Africa 2023. GSMA Intelligence. https://www.gsma.com

Hatlevik, O. E., Throndsen, I., Loi, M., & Gudmundsdottir, G. B. (2022). Exploring digital literacy: Skills, safety, and problem-solving in digital environments. Computers & Education, 179, 104425.

Ibrahim, L., Mohammed, A., & Shehu, Y. (2023). Socio-economic barriers to cybersecurity adoption in low-income communities. African Journal of ICT Development, 7(2), 54–69.

Jibunoh, C., Eze, P., & Ali, S. (2024). Emerging cybersecurity threats in low-income African communities: The rise of mobile malware and cryptojacking. International Journal of Cyber Threat Analysis, 9(1), 22–39.

Kaspersky. (2021). Global cybersecurity awareness report 2021. Kaspersky Security Research. https://www.kaspersky.com

Nweke, C., & Okolo, F. (2023). Socio-cultural determinants of cybersecurity practices in rural Nigerian communities. Journal of African Cyber Policy Studies, 6(2), 88–104.

Okeke, D., Nnaji, C., & Eze, R. (2022). Cybersecurity awareness gaps among underserved populations in Nigeria. Nigerian Journal of Information Security, 4(1), 15–29.

Olowu, A. (2020). Cybersecurity awareness and challenges among underserved users in Sub-Saharan Africa. African Journal of Information Security, 3(2), 20–35.

Park, Y., & Kim, H. (2022). Perceptions of cybersecurity risk among low-literate populations in rural South Korea. Journal of Cybersecurity Education and Research, 14(1), 61–75.

Uche, M., Omondi, P., & Wanjiru, J. (2023). Community-based cybersecurity awareness strategies in Kenya: A participatory approach. East African Journal of Information Systems, 9(2), 101–118.

Yusuf, A., Musa, L., & Bello, K. (2022). Cybersecurity awareness and digital literacy in Northern Nigeria: An empirical study. Journal of ICT and Society, 11(4), 77–92.