A Localized SMS Scam Alert System for the Elderly and Digitally Inexperienced Users in Benue State, Nigeria

[1]Samera U. Otor, [2]Chiangi Terlumun, [3]Joseph S. Idikwu and [4]Beatrice O. Akumba
[1,2,3,4]Department of Mathematics and Computer Science, Rev. Fr. Moses Orshio Adasu University formerly known as Benue State University, Makurdi, Nigeria
sotor@bsum.edu.ng | chiangiterlumun@gmail.com | josephinnocent99@gmail.com | beatriceobianiberi@gmail.com

Received: 05-MAY-2026; Reviewed: 17-JUNE-2026; Accepted: 10-AUGUST-2026
https://dx.doi.org/10.46792/fuoyejet.v11i3.1576

ORIGINAL RESEARCH

Abstract— In today's digital landscape, the rise in cyber threats, particularly electronic message scams have become a critical concern. Cyber fraud incidents have surged globally, resulting in financial losses, psychological distress among victims and reduced trust in digital communication. Individuals with limited technological awareness are highly vulnerable to scam messages and fraudulent calls. Recently, scam messages have become more sophisticated, exploiting emotional intelligence to manipulate people's' conscience, thereby requiring advanced measures to detect them. Consequently, conventional cybersecurity measures often require advanced technical knowledge, making them ineffective for this demographic. Hence, this study presents the development of a Cybersecurity Awareness System designed to identify and alert the elderly and non-tech-savvy about fraudulent SMS messages. The system integrates a structured database of known scam messages and translated them into local dialects (Tiv, Idoma and Igede) to enhance comprehension. The system was implemented using HTML, CSS, PHP, MySQL and JavaScript, with XAMPP serving as the development environment. Simulation was achieved through a controlled test environment, ensuring real-world applicability. The simulation module, visually displays received scam messages on a simulated web-based handset screen. The system's performance was evaluated, demonstrating an accuracy of 97%, precision of 96.1%, recall (sensitivity) of 98% and an F1-Score of 97% in the detection and classification of scam messages. These results confirm the system's effectiveness in promptly identifying and warning users about fraudulent communications. The study highlights the importance of localized cybersecurity awareness tools and recommends further enhancements, including AI-driven scam detection and broader language integration, to strengthen digital security for vulnerable populations.

Keywords—Cybersecurity, Scam messages, The Elderly, Localized SMS, Non-tech-savvy.

1 INTRODUCTION

The advent of the digital age has revolutionized communication and information sharing. However, it has also created opportunities for cybercriminals to exploit unsuspecting individuals through malicious activities such as phishing, scam calls and fraudulent SMS messages. Elderly populations, particularly those in rural areas, are disproportionately affected due to their limited exposure to technology and cybersecurity education (Karagiannopoulos et al., 2021).

In Benue State, Nigeria, a region with predominantly rural population and diverse groups such as Tiv, Idoma and Igede, the elderly and digitally unaware are especially vulnerable. Many rely on basic feature phones for communication, often unaware of the dangers posed by scam messages and fraudulent calls. Cybercriminals exploit this vulnerability through social engineering tactics, using urgent or familiar language to deceive or emotionally coerce their victims (Alhogail & Alsabih 2021). A typical example involves scam calls or SMS from impostors pretending to be relatives in distress, urgently requesting financial help. Such incidents often leave victims psychologically disturbed making them respond without verification (Alhogail & Alsabih 2021). At its core, cybersecurity is about safeguarding systems, networks and personal information from threats like hacking, phishing and malware. For the elderly and non-tech savvy, this protection requires not only technology but also education and essential tool to empower them to recognize and avoid cyber threats. Cybercriminals frequently rely on social engineering, manipulating emotions such as fear and trust to carry out their schemes. Strategies like impersonation scams, where attackers pose as trusted individuals and urgency-based scams, which prompt immediate action, are particularly employed. Unfortunately, elderly individuals in rural areas, unfamiliar with fraud prevention measures, are easy targets for such attacks (Saifuddin et al., 2024).

One of the most common methods used by cybercriminals in this region is the delivery of scam messages and fraudulent calls. These messages often claim false rewards, block access to accounts, or demand urgent financial aid. They are crafted in English, which poses another challenge for many elderly residents who primarily speak Tiv, Idoma, or Igede. Examples include alarming texts stating, "Your ATM card has been blocked. Send your BVN to reactivate it," or manipulative pleas such as "Hello Mama, it's me, your son! I need money urgently, I am sick. Please send it now." With limited digital knowledge, many elderly individuals and non-tech savvy, struggle to identify these as fraudulent, falling victim to them and losing significant sums of money (Steinmetz et al., 2024). Recognizing these challenges, cybersecurity awareness initiatives have attempted to fill the gap. However, most of these programs are designed for urban, literate populations, delivered in English, effectively excluding many elderly residents of rural areas and non-tech-savvy. This language barrier leaves them unable to

Corresponding Author:
Section B- ELECTRICAL/COMPUTER ENGINEERING & RELATED SCIENCES
Can be cited as:
Otor S. U., Terlumun C., Idikwu J. C., and Akumba B. O. (2026). A Localized SMS Scam Alert System for the Elderly and Digitally Inexperienced Users in Benue State, Nigeria. FUOYE Journal of Engineering and Technology (FUOYE**JET**), **11(3), 392-397.** https://dx.doi.org/10.46792/fuoyejet.v11i3.1576

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

access crucial information needed to protect themselves from cyber threats (Mustapha &, Alabi, 2022). To address this issue, a tailored solution is proposed: a cybersecurity awareness platform specifically designed for the elderly population and non-tech savvy in Benue State. This system would use SMS-based alerts to educate users about the nature of scam messages. It provides multilingual translations of common scams into Tiv, Idoma and Igede, enabling better understanding and protection. For a message such as "Your bank account has been blocked. Send your BVN to reactivate it," the platform can translate it into any of the three major indigenous languages of Benue State, along with a corresponding warning alert like, "This is a scam. Do not reply or share your BVN. Contact your bank directly." By creating such an innovative and localized tool, this initiative bridges the gap and enables the elderly and non-tech-savvy to navigate the digital world with confidence. With its multilingual approach and focus on their unique vulnerabilities, this system has the potential to transform their ability to respond to cyber threats, ultimately reducing their risk and restoring peace of mind.

2 LITERATURE REVIEW

Despite the increasing global efforts to improve cybersecurity awareness, cyber fraud remains a persistent and evolving threat, particularly among vulnerable populations such as the elderly in rural communities. The rapid expansion of mobile communication technologies has created new opportunities for cybercriminals to exploit users through smishing (SMS phishing), impersonation scams and fraudulent SMS messages. Alhogail & Alsabih (2021) observed that while technological defenses continue to advance, human vulnerability remains one of the weakest links in cybersecurity frameworks. They emphasize that awareness and behavioral education are critical components in reducing successful cyberattacks.

Early cybersecurity awareness initiatives primarily targeted corporate environments, focusing on technical safeguards such as firewalls, antivirus software and password management systems (Bada et al., 2019). However, the proliferation of mobile devices shifted the attack surface toward individual users. Hart et al. (2020) noted that scam messages increasingly exploit emotional triggers such as urgency, fear and greed, particularly targeting the elderly or users who may lack digital literacy skills. These scams often involve impersonation of financial institutions, fake lottery winnings, or urgent account suspension warnings. Research has increasingly emphasized SMS-based awareness interventions as effective tools for reaching populations with limited internet access. Netshiunda and Madzvamuse (2025) reported that SMS-based awareness systems provide an effective medium for communicating cybersecurity information in areas with limited internet infrastructure and low smartphone adoption. Their findings showed improved access to security information and timely dissemination of alerts. Nevertheless, their approach focused primarily on message delivery efficiency and did not adequately address language barriers that affect comprehension among elderly users.

Language has also emerged as a crucial factor in cybersecurity education. Egere et al. (2025) found that delivering awareness messages in native dialects substantially improved comprehension and behavioral response among rural populations. Their study revealed that localized cybersecurity education enhanced retention and reduced susceptibility to phishing attacks compared to programs delivered in formal languages. Although the study validated language localization as an effective strategy, it did not integrate a practical SMS simulation environment specifically designed for elderly populations using basic mobile phones. These findings support the integration of Tiv, Idoma and Igede dialects in SMS-based awareness systems targeting elderly and non-literates in Benue State. Behavioral economics has further influenced cybersecurity awareness strategies. Arciulo & Di Nocera, (2026) highlighted the effectiveness of nudging techniques, where periodic reminders and simplified instructions encourage secure behaviors without restricting user choice. Their research suggests that continuous reinforcement through short, actionable messages significantly improves cybersecurity habits, particularly among individuals with low digital literacy. Empirical evidence from rural and developing communities further underscores the vulnerability of users, as cybercrime victims are often influenced by low digital literacy, economic pressure and limited cybersecurity awareness (Egere et al., 2025). Studies have shown that individuals possessing higher levels of digital literacy are less likely to fall victim to phishing attacks due to their improved ability to recognize fraudulent messages. Furthermore, structured cybersecurity awareness and training interventions have been shown to significantly improve users' ability to detect phishing and scam messages (Jampen et al., 2020). Multilingual and context-aware cybersecurity communication has also been found to enhance user understanding and engagement, particularly among populations with limited access to formal digital education (Ahmed & Mejri, 2025). Multilingual cybersecurity campaigns have demonstrated measurable impact, as research shows that message comprehension significantly affects users' ability to detect fraudulent SMS and phishing attempts, especially in low-literacy environments (Awumee et al., 2023). Collectively, these studies confirm the value of language-sensitive awareness approaches but reveal insufficient attention to indigenous-language implementation for rural elderly populations.

Studies on SMS-based cybercrime systems further reveal that structured awareness messages delivered through mobile communication channels improve user engagement and threat recognition in vulnerable populations (Salman et al., 2022). Additionally, research on cybersecurity awareness training systems highlights that user understanding of phishing and scam messages strongly influences detection accuracy and behavioral response, emphasizing the importance of clear and context-aware communication in cybersecurity education (Hart et al., 2020). Although these

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

http://dx.doi.org/10.46792/fuoyejet.v11i3.1576 engineering.fuoye.edu.ng/journal

studies validated mobile communication as an effective awareness mechanism, they did not specifically target users who depend exclusively on feature phones and indigenous communication channels.

Technological solutions for scam detection have also advanced considerably. Catal et al. (2022) demonstrated that machine learning techniques achieved high performance in detecting phishing and fraudulent messages. Likewise, Alkhalil et al. (2021) concluded that integrating AI-based detection with cybersecurity awareness significantly reduced phishing success rates. While these technological solutions show strong detection capabilities, they often require computational resources, internet connectivity and technical infrastructure that may not be feasible in rural communities with low digital accessibility. At the policy level, national cybersecurity frameworks have sought to improve public awareness and strengthen cyber resilience. Aldaajeh et al. (2022) emphasized that awareness initiatives produce measurable benefits only when implementation strategies align with users' social and technological realities. Schiliro (2023) further identified implementation challenges that limit practical policy effectiveness across different environments. Similarly, Quayyum and Freberg (2023) highlighted the absence of culturally and linguistically inclusive cybersecurity awareness frameworks in developing regions. These findings reinforce the argument that awareness systems must incorporate local communication patterns and language diversity to achieve meaningful outcome. While substantial research exists on cybersecurity awareness, few studies focus specifically on elderly rural populations who rely on basic mobile phones and communicate primarily in indigenous dialects. Many existing interventions depend on formal languages, limiting comprehension. Therefore, there remains a critical need for a localized SMS-based cybersecurity awareness system tailored to the elderly and non-tech literate users. The present study addresses this gap by developing a culturally and linguistically adapted awareness system designed to improve scam recognition and mitigate cyber threats among individuals in Benue State.

3 METHODOLOGY

This study adopted a system design and development methodology, that encompasses system formulation, database design, simulation, and performance evaluation.

1. System Representation and Formulation

Let the set of complete SMS messages be:

$$M = \{m_i \dots m_n\} \quad (1)$$

where,

M = the set of all scam messages collected.

$\{m_i \dots m_n\}$ = individual messages in the set.

Let

$$m_i = (x_1, x_2 \dots x_k) \quad (2)$$

m_i: represents the ith message in the data set

x_1: the first feature extracted from the message (e.g urgency indicator)

x_2: the second feature extracted from the message (e.g impersonation key word)

x_k: the kth feature extracted from the message (final feature in the set)

Let

$$y \in \{0,1\} \quad (3)$$

Be the classification indicator, where:

$y = 1$ represents a scam message

$y = 0$ represents a legitimate message

Since the proposed system is rule-based, a detection function $D(m_i)$ was developed using predefined scam patterns and keyword validation rules where $D(m_i)$ =1 if $m_i \in M$ and $D(m_i)$ =0 if $m_i \notin M$.

The classification process is expressed as:

$$D(m_i) = y \quad (4)$$

This is a detection function to check each message and decide its category.

The system takes a message $D(m_i)$ as input, It produces an output y, which shows the result of the classification. If

$y = 1$ The message is a scam

$y = 0$ The message is legitimate (safe

Following detection, a localization function was designed to translate scam messages into indigenous dialects as follows

$$T = (t_1, t_2, t_3) \quad (5)$$

Represent supported dialects where:

t_1= Tiv

t_2 = Idoma

t_3 = Igede

The translation output is defined as:

$$L(m_i, t_j) \rightarrow T(w_i) \quad (6)$$

where, L and T are the localization and the translation generated for a selected message $m_i$and dialect $t_j$respectively. To integrate detection and localization, the overall awareness function is a composition function defined as:

$$T(w_i) = \{D(m_i), L(m_i, t_j)\} \quad (7)$$

where, $T(w_i)$ = final system output consisting of detection and translated warning alert.

All processed transactions are recorded. This ensures traceability and monitoring of all simulated message transactions to enable evaluation.

2. Database Design

The system database was designed using MySQL. Two primary tables were designed:

scam_message table – Stores original English scam messages, Tiv translation, Idoma translation, Igede translation and their corresponding warning alerts.

sms_logs table – Stores recipient name, phone number, selected dialect, message sent and timestamp.

If a scam message is not found in the database, the system allows manual insertion and immediate storage for future retrieval.

3. System Simulation

The developed awareness system was simulated using collected scam messages obtained from:

Telecommunication reports, interviews with victims, online scam awareness platforms among others.

The operational process includes:

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.

This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)
http://dx.doi.org/10.46792/fuoyejet.v11i3.1576 engineering.fuoye.edu.ng/journal

1. User authentication
2. Recipient detail entry
3. Dialect selection (Tiv, Idoma, Igede)
4. Scam message retrieval
5. Translation and warning alert display
6. SMS simulation rendering
7. Transaction logging

The system was implemented using:
Frontend: HTML, CSS, JavaScript
Backend: PHP
Database: MySQL
Server Environment: XAMPP

4. Performance Evaluation

Although the system is rule-based, its effectiveness was evaluated using standard classification metrics.

$$Accuracy = (TP + TN) / (TP + TN + FP + FN) \quad (8)$$

$$Precision = TP / (TP + FP) \quad (9)$$

$$Recall = TP / (TP + FN) \quad (10)$$

$$F1 - Score = 2 \times (Precision \times Recall) / (Precision + Recall) \quad (11)$$

Where:
TP = True Positives (correctly identified scam messages)
TN = True Negatives (correctly identified legitimate messages)
FP = False Positives (legitimate messages flagged as scam)
FN = False Negatives (scam messages not detected)

These metrics quantify the reliability and detection accuracy of the developed awareness system.

4 RESULTS AND DISCUSSIONS

4.1 SYSTEM IMPLEMENTATION RESULTS

1. User Registration Module

The registration module enables new users to create an account by providing their name, email address and password. Email validation was implemented to prevent duplicate registrations, while passwords were encrypted before storage in the database to enhance security.

The system successfully validates user input and prevents duplicate email entries as shown in Figure 1

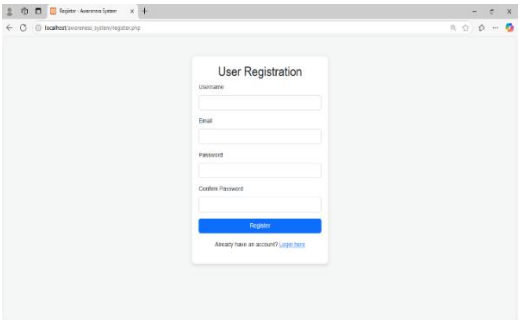

Fig. 1. Screenshot of user registration form.

2. User Authentication Module

The login module ensures that only authorized users can access the system dashboard. Users are required to enter valid credentials (email and password). Upon successful authentication, a session is initiated to maintain secure access. Invalid login attempts trigger an error message, preventing unauthorized access. Session management was effectively implemented to maintain authentication integrity as shown in Figure 2

3. Scam Message Sending Module

The message sending module enables authorized users to select predefined scam messages stored in the database and send them along with translated warning alerts based on the recipient's tribe (Tiv, Idoma, or Igede).The system dynamically retrieves scam messages and corresponding translations from the database as shown in Figure 3.

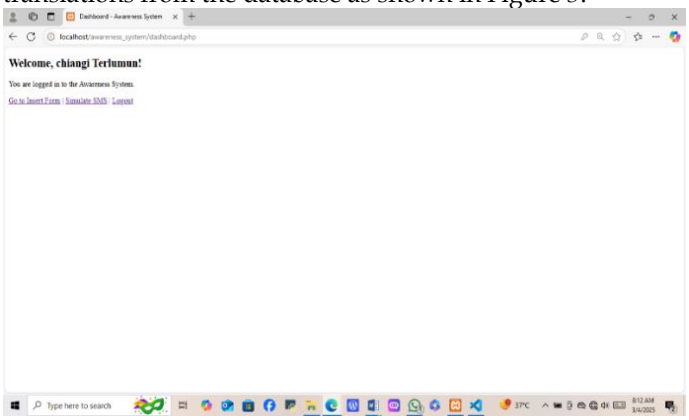

Fig. 2. Screenshot of successful login to the Awareness System.

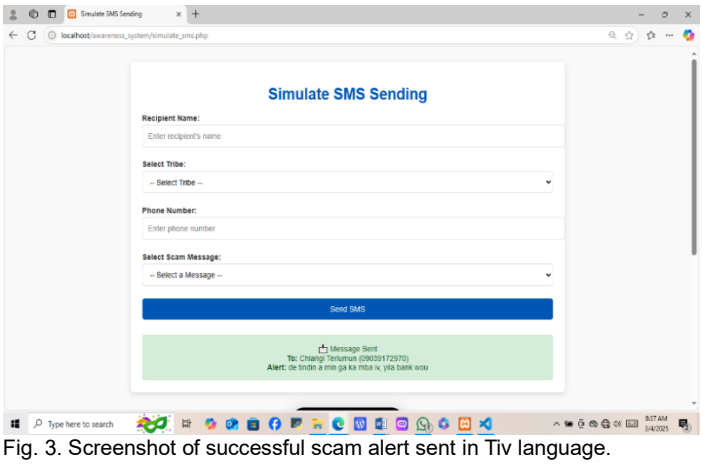

Fig. 3. Screenshot of successful scam alert sent in Tiv language.

4. SMS Simulation Module

5. Fig. 4. Screenshot of successful message simulation

The SMS simulation module visually replicates how a scam message appears on a recipient's mobile device. The system displays:
The original scam message

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

The translated warning alert
Advisory instructions (e.g., ignore or report the message) as shown in Figure 4.
The successful integration of translation and simulation significantly improves scam awareness among non-English-speaking elderly individuals.

4.2. System Performance Evaluation Results

The evaluation results for Precision, Recall, Accuracy and F1-Score for 50 scam messages and 50 legitimate messages are as presented in Table 1 and Figure 5 respectively.

Table 1. Confusion Matrix of evaluation Result.

		Predicted scam	legitimate
Actual	Scam	TP=49	FN= 1
	Legitimate	FP= 2	TN= 48

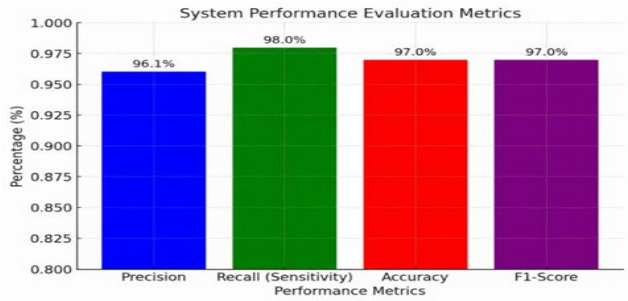

Fig. 5. Graphical representation of system performance evaluation.

The system achieved an accuracy of 97%, indicating that most of the scam messages were correctly classified. The precision value of 96.1% demonstrates that the system minimizes false alerts to 4%, ensuring that only verified scam messages are transmitted. A recall of 98% indicates that the system successfully identifies and processes the majority of stored scam messages omitting only 2. The F1-score of 97% reflects a strong balance between precision and recall, confirming the system's reliability in delivering relevant awareness notifications. Overall, the results demonstrate the potential effectiveness under controlled conditions in mitigating scam-related risks among users.

5 Conclusion

This study presented the design and implementation of a Cybersecurity Awareness System developed to mitigate scam attacks targeting elderly people and non-tech savvy individuals in Benue State. The study developed a structured framework capable of storing documented scam messages, translating them into Tiv, Idoma and Igede languages and generating awareness alerts to enhance fraud recognition among users.
The system integrates a secure user management module, structured scam message categorization, language translation support and SMS simulation to provide a comprehensive awareness mechanism. By incorporating localized language translation, the system bridges the communication gap that often expose users with limited digital literacy to cyber fraud due to limited English proficiency.
Performance evaluation was conducted using standard metrics including precision, recall, accuracy and F1-score. The system achieved an accuracy of 97%, with precision, recall and F1-score values of 96.1%, 98% and 97% respectively. The high accuracy confirms that scam messages were correctly classified before alert transmission. The precision value indicates minimal false alerts, ensuring reliability and user trust, while the recall score demonstrates that most relevant scam patterns were successfully captured. The balanced F1-score further validates the robustness and consistency of the system. The analysis of scam patterns revealed that impersonation scams are the most prevalent fraud category affecting elderly individuals in Benue State. Fraudsters commonly exploit urgency and emotional attachment by posing as relatives or trusted individuals. The structured categorization of these scam types enables the system to generate targeted warnings aligned with dominant fraud patterns. Future enhancements should incorporate Artificial Intelligence (AI) techniques to enable automated scam pattern recognition. The integration of NLP could enable the system to dynamically analyze incoming SMS content, particularly as Tiv translation tools already exist, while Idoma and Igede translators can be developed to further broaden the system's reach and generate intelligent warnings without relying solely on pre-stored templates.
In addition, the development of an AI-powered voice alert system in Tiv, Idoma and Igede languages would significantly enhance accessibility for illiterate elderly users. Such integration would allow the system to convert scam warnings into spoken alerts, ensuring inclusiveness across different literacy levels. Collaboration with cybersecurity agencies and network providers is also recommended to enable real-time reporting and blocking of fraudulent phone numbers. Expanding the system to incorporate additional Nigerian languages will further broaden its impact and scalability. With the integration of AI-driven detection mechanisms and voice-based intelligent alerts, the system will have a strong potential to evolve into a comprehensive national cybersecurity awareness framework.

References

Ahmed, A. M., & Mejri, M. (2025). Generative AI for cybersecurity awareness training. In Proceedings of IECON 2025, 1–10. https://doi.org/10.1109/iecon58223.2025.11221870

Alhogail, A., & Alsabih, A. (2021). Applying machine learning and natural language processing to detect phishing email. *Computers & Security, 111*, 102414. https://doi.org/10.1016/j.cose.2021.102414

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3, 563060. https://doi.org/10.3389/fcomp.2021.563060

Arciulo, L., & Di Nocera, F. (2026). The nudging paradigm in cybersecurity research: A PRISMA-based systematic review. *Information*, 17(3), 264. https://doi.org/10.3390/info17030264

Awumee, G. S., Agyemang, J. O., Bempong, D., & Ansong, E. D. (2023). SmishShield: A machine-learning-based smishing detection system.

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

2023, Lecture Notes on Data Engineering and Communications Technologies The 6th International Conference on Wireless, Intelligent and Distributed Environment for Communication, Springer Nature Switzerlandp. 205-221 https://doi.org/10.1007/978-3-031-47126-1_14

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv. https://doi.org/10.48550/arXiv.1901.02672

Aldaajeh, S. H., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K.-K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security, 119(4),* 102754. https://doi.org/10.1016/j.cose.2022.102754

Catal, C., Giray, G., Tekinerdogan, B., Kumar, S., & Shukla, S. (2022). Applications of deep learning for phishing detection: A systematic literature review. *Knowledge and Information Systems*, 64, 1457–1500. https://doi.org/10.1007/s10115-022-01672-x

Egere, A. N., Adamu, A. Y., & Nwokocha, A. (2025). Community-centric cybersecurity education for low-literacy users in Northeast Nigeria. *Journal of Science Innovation and Technology Research, 9*(9). https://doi.org/10.70382/ajsitr.v9i9.045

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cybersecurity awareness and education. *Computers & Security*, 95, 101827. https://doi.org/10.1016/j.cose.2020.101827

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: Towards an effective anti-phishing training.A Comparative literature review *Human-Centric Computing and Information Sciences*, 10(33), 1-41. https://doi.org/10.1186/s13673-020-00237-7

Karagiannopoulos, V., Kirby, A., Oftadeh-Moghadam. S., & Sugiura, L. (2021).Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study. *Computer Law & Security Review*, 43, 105615. https://doi.org/10.1016/j.clsr.2021.105615

Mustapha, S. D., & Alabi, A. A. (2022). Advancing cybersecurity awareness programs: A model for sustainable digital literacy in underserved communities. *Journal of Multidisciplinary Studies*, 3(2), 111–128. https://doi.org/10.53022/oarjms.2022.3.2.0048

Netshiunda, H., & Madzvamuse, S. (2025). A systematic literature review of cybersecurity awareness and strategy in rural-based universities. International Journal of Applied Research in Business and Management, 6(5). https://doi.org/10.51137/wrp.ijarbm

Quayyum, F., & Freberg, G. N. (2023).Designing cybersecurity awareness solutions for young people in rural developing countries: The need for diversity and inclusion. arXiv. https://doi.org/10.48550/arXiv.2312.12073

Saifuddin, N. F., Musa, B., Zakaria, N. S., Othman, N. F., Putera, A. D., Kunasekaran, P., Rosnon, M. R., Razak, M. A. A., & Ibrahim, R. (2024). Scams Issues among Elderly: A Conceptual Paper. International Journal of Academic Research in Business and Social Sciences, 14(10), 1624–1634. http://dx.doi.org/10.6007/IJARBSS/v14-i10/23268

Salman, M., Ikram, M., & Kaafar, M. A. (2022). An empirical analysis of SMS scam detection systems. arXiv. https://doi.org/10.48550/arXiv.2210.10451

Schiliro, F. (2023). Building a resilient cybersecurity posture: A framework for leveraging prevent, detect and respond functions and law enforcement collaboration. arXiv. https://doi.org/10.48550/arXiv.2303.10874

Steinmetz, K. F., Holt, T. J., & Brewer, C. G. (2024). Developing and implementing social engineering-prevention policies: A qualitative study. *Security Journal*, 37(3), 599–617. https://doi.org/10.1057/s41284-023-00385-2

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)