*International Journal of Linguistics and computational Applications (IJLCA)* ISSN 2394-6385(Print)
*Volume 13, Issue 2, April – June 2026* ISSN 2394-6393(Online)

# Cyber Security Awareness among Zambian Citizens: AI-Driven Digital Literacy, Threat Education and National Cyber Resilience Strategies

Wabei Kekelwa[*1], Dr. Ravibaskar Ramalingam[2]

[1]*Student, DMI St. Eugene University, Zambia*
[2]*Associate Professor, DMI St. Eugene University, Zambia*

***Abstract*** —As digital technology penetrates more deeply into Zambian civic and economic life through mobile money, e-government services, social media, and online commerce cybersecurity awareness among citizens has become a national development imperative. Low cybersecurity awareness creates vulnerability to phishing, identity theft, online fraud, social media manipulation, and ransomware risks that disproportionately affect the most digitally inexperienced users, including rural communities, elderly citizens, and those newly entering the digital economy. This article investigates cybersecurity awareness among Zambian citizens, contextualising findings within global scholarship on national cybersecurity strategy, AI-driven threat education platforms, digital literacy development, and community-based cyber resilience programmes. Drawing on a survey involving 10 ICT experts and broader citizen assessment, findings reveal that awareness of common cybersecurity threats is low, safe online behaviour practices are inconsistently adopted, and institutional support for cybersecurity education is fragmented and insufficient. AI-powered cybersecurity training platforms, national digital literacy programmes, and community-based cyber awareness campaigns are identified as evidence-based pathways for improving national cyber resilience. Policy recommendations are presented.

***Keywords*** *— Cybersecurity Awareness; Digital Literacy; Zambia; AI Security Training; National Cyber Resilience; Online Safety; Citizen Education.*

## 1. Introduction

Cybersecurity the protection of digital systems, networks, and data from unauthorised access, manipulation, and disruption has become a foundational concern for individuals, institutions, and governments in the digital age (Venice et al., 2025f; Vettriselvan et al., 2025c). For Zambia, where mobile phone penetration now exceeds 60% and digital financial services including mobile money and internet banking are progressively displacing cash transactions, cybersecurity threats represent a growing source of financial and personal harm for citizens whose awareness of digital risks has not kept pace with their digital technology adoption (Venice et al., 2025b; Vettriselvan et al., 2025b).

Social engineering attacks including phishing emails, SMS scams, and social media fraud exploit psychological vulnerabilities rather than technical weaknesses, making citizen awareness and behavioural knowledge the primary defence against the most prevalent cybersecurity threats (Venice et al., 2025a; Basha et al., 2025). AI-powered cybersecurity training platforms, digital literacy programmes, and community-based cyber awareness campaigns offer evidence-based pathways for building the citizen cybersecurity knowledge and safe online behaviour practices that constitute national cyber resilience (Venice et al., 2025f; Vasantha et al., 2025). This article investigates Zambian citizen cybersecurity awareness and identifies strategies for national cyber resilience building.

## 2. Literature Review

### 2.1 Cybersecurity Threats and Citizen Vulnerability

The threat landscape facing ordinary citizens in digital economies encompasses phishing attacks that harvest login credentials and financial data through deceptive communications, identity theft through social media information exploitation, online financial fraud through fake merchant sites and investment scams, and social media manipulation through disinformation and fake account interactions (Venice et al., 2025f; Basha et al., 2025). In Zambia, mobile money fraud including SIM swap attacks, fraudulent agent impersonation, and social engineering of account credentials represents a particularly prevalent and financially damaging cybersecurity threat given the high penetration and primary financial role of mobile money services (Venice et al., 2025b; Vettriselvan et al., 2025c). Low cybersecurity awareness among citizens particularly those who are new digital adopters without prior exposure to digital risk education creates systematic vulnerability to these threats regardless of the technical security measures implemented by service providers (Venice et al., 2025a; Vinodh et al., 2026a; Aneeshkumar et al., 2024). Social vulnerability to cybersecurity threats intersects with broader social vulnerability patterns: elderly citizens, those with lower education levels, rural communities with limited access to cybersecurity information, and citizens newly accessing digital services for the first time are disproportionately represented among cybercrime victims


DOI: 10.30726/ijlca/v13.i2.2026.132008

(Ashifa, 2022; Kariveliparambil et al., 2026b). Gender dimensions of cybersecurity vulnerability are also significant with women facing elevated risks of online harassment, intimate image abuse, and gender-targeted financial scams (Ashifa et al., 2019; Vettriselvan & Anto, 2018).

### 2.2 AI-Driven Cybersecurity Education and Training

AI-powered cybersecurity training platforms offer significant potential for building citizen cybersecurity awareness at population scale in cost-effective, contextually adaptive formats (Venice et al., 2025f; Akila et al., 2025). Adaptive learning systems that assess individual user cybersecurity knowledge profiles and deliver personalised training content focusing on the specific threat types and risk behaviours most relevant to each user's digital activity patterns ensure that training is targeted to actual individual risk rather than generic content that may be irrelevant or redundant for many users (Venice et al., 2025b; Vasantha et al., 2025). Gamified cybersecurity training applications that simulate phishing attacks, social engineering scenarios, and password security challenges in engaging, consequence-free environments build threat recognition skills through experiential learning that lecture-format awareness programmes cannot replicate (Venice et al., 2025c; Swadhi et al., 2025a). AI-powered threat intelligence systems that monitor local and national cybercrime patterns identifying emerging scam types, new attack vectors, and seasonal fraud trends can generate targeted public alerts that keep citizen awareness current with rapidly evolving threat landscapes (Venice et al., 2025a; Devi et al., 2025). Natural language processing systems that automatically translate cybersecurity guidance into local languages, at appropriate literacy levels, ensure that awareness content is accessible to the full range of Zambian citizens regardless of English literacy level (Venice et al., 2025d; Arockia et al., 2025).

### 2.3 National Cybersecurity Strategy and Policy

Effective national cybersecurity awareness requires a coordinated policy framework encompassing regulatory requirements for digital service providers, national digital literacy curriculum integration, mass public awareness campaign infrastructure, and cross-sector partnerships between government, telecommunications companies, financial institutions, and civil society (Venice et al., 2025f; Vinodh et al., 2026a). Zambia's National Cybersecurity Policy and associated legislation provide a regulatory foundation for national cybersecurity governance but citizen awareness education components of this framework require significantly stronger implementation, particularly in rural and underserved communities (Vettriselvan et al., 2025d; Venice et al., 2025b). Blockchain-enabled incident reporting and cybercrime statistics systems that generate transparent, real-time national cybersecurity threat dashboards provide both policy makers and citizens with accurate information about the scale and nature of cybercrime risk building the evidence base for targeted awareness investment (Rajeswari et al., 2026; Venice et al., 2025c).

### 2.4 Community-Based Cyber Awareness and Digital Citizenship

Community-based cyber awareness programmes delivered through trusted community institutions including schools, churches, community centres, and local government offices have demonstrated effectiveness in reaching digitally inexperienced citizens who are not accessible through conventional online awareness channels (Kariveliparambil et al., 2026a; Rasi & Ashifa, 2019). Digital citizenship education integrated into civic education curricula from primary through to secondary level builds the foundational online safety knowledge, critical evaluation skills, and safe behaviour habits that provide lifelong cyber resilience (Vijayalakshmi et al., 2025a; Venice et al., 2025f). Peer cyber safety education networks training community members to serve as local cybersecurity awareness champions who educate their networks extend awareness programme reach through trusted

## 3. Methodology

A descriptive survey was employed to investigate cybersecurity awareness among Zambian citizens. Mixed methods combined structured questionnaires administered to a diverse citizen sample, in-depth interviews with 10 ICT and cybersecurity experts, and analysis of available national cybersecurity incident data (Kombo & Tromp, 2014; Orodho & Kombo, 2012). The citizen sample comprised 80 participants drawn across urban and rural strata, gender, age groups, and education levels. Data collection instruments measured cybersecurity threat knowledge, safe online behaviour practice, personal cybercrime experience, and awareness education exposure. Expert interviews explored national threat landscape and education policy. Thematic analysis and descriptive statistics were applied.

## 4. Findings and Analysis

### 4.1 Cybersecurity Awareness Levels

Citizen cybersecurity awareness assessment revealed significant knowledge gaps across all threat categories: only 42% could correctly identify a phishing email from a described example; 35% were aware of SIM swap fraud risks despite widespread mobile money use; and 28% practised password security behaviours (unique passwords,


DOI: 10.30726/ijlca/v13.i2.2026.132008

regular changes, non-sharing). Rural respondents demonstrated significantly lower awareness than urban counterparts across all measured dimensions a digital risk equity gap with particular significance given rural communities' increasing digital financial inclusion through mobile money (Venice et al., 2025b; Vasantha et al., 2025).

### 4.2 Cybercrime Victimisation Experience

Direct cybercrime victimisation was reported by 38% of respondents primarily mobile money fraud (65% of victimised respondents), social media account compromise (22%), and online shopping fraud (13%). Expert interviewees estimated that actual victimisation rates significantly exceed reported rates due to stigma, limited law enforcement responsiveness, and uncertainty about where to report incidents (Venice et al., 2025f; Basha et al., 2025).

### 4.3 Awareness Education Exposure

Prior cybersecurity awareness education was reported by only 25% of respondents, primarily from employer training (35% of educated respondents), social media content (30%), and school or university programmes (20%). Community-based awareness programmes had reached fewer than 10% of respondents. ICT expert interviewees identified the absence of a national mass citizen cybersecurity awareness campaign as a critical gap in Zambia's cyber resilience strategy (Venice et al., 2025a; Vinodh et al., 2026a).

### 4.4 Preferred Awareness Channels

Preferred cybersecurity awareness channels identified by respondents included mobile phone SMS campaigns (78%), radio programmes in local languages (72%), community organisation workshops (65%), and mobile application-based training (55%). These preferences confirm the potential of mobile-first, community-mediated awareness approaches in the Zambian context (Venice et al., 2025b; Arockia et al., 2025).

## 5. Discussion

The low cybersecurity awareness documented among Zambian citizens creates a significant and growing national security risk as digital service adoption continues to expand. The gap between digital technology adoption and cybersecurity awareness education where citizens are rapidly engaging with digital financial services without corresponding safety knowledge represents a systematic policy failure that demands urgent national attention (Venice et al., 2025f; Vasantha et al., 2025). AI-powered mobile cybersecurity training platforms, delivered in local languages and calibrated to diverse user digital literacy levels, offer the most scalable and cost-effective pathway for rapidly expanding citizen cybersecurity awareness across Zambia's heterogeneous digital landscape (Venice et al., 2025b; Akila et al., 2025; Arockia et al., 2025).

## 6. Conclusion and Recommendations

Recommendations: (1) launch a national AI-powered mobile cybersecurity awareness campaign in local languages (Venice et al., 2025b; Arockia et al., 2025); (2) integrate cybersecurity and digital citizenship education into national school curricula from primary level (Vijayalakshmi et al., 2025a; Venice et al., 2025f); (3) train community cyber safety champions in rural areas to extend awareness reach (Kariveliparambil et al., 2026a; Vettriselvan et al., 2026b); (4) establish blockchain-enabled national cybercrime reporting and statistics platforms (Rajeswari et al., 2026; Venice et al., 2025c); and (5) mandate cybersecurity awareness training for all digital financial service users at account registration (Venice et al., 2025a; Vinodh et al., 2026a).

## References

[1] Akila, V., Prabhu, G., Akila, R., & Swadhi, R. (2025). Performance metrics in blockchain-enabled AIML for cognitive IoT in large-scale networks. In AI for large scale communication networks (pp. 265–288). IGI Global Scientific Publishing.

[2] Arockia, V. J., Vettriselvan, R., Rajesh, D., Velmurugan, P. R. R., & Cheelo, C. (2025). Leveraging AI and learning analytics for enhanced distance learning. In AI and learning analytics in distance learning (pp. 179–206). IGI Global Scientific Publishing.

[3] Ashifa, K. M. (2019). Developmental initiatives for persons with disabilities. Indian Journal of Public Health Research & Development, 10(12), 1257–1261.

[4] Ashifa, K. M. (2020a). Effect of substance abuse on physical health of adolescents. European Journal of Molecular & Clinical Medicine, 7(2), 3155–3160.

[5] Ashifa, K. M. (2020b). Physical health hazards of schizophrenia patients. Systematic Reviews in Pharmacy, 11(12), 1848–1850.

[6] Ashifa, K. M. (2021a). Analysis on the determinants of health status among tribal communities. Journal of Cardiovascular Disease Research, 12(3), 531–534.

[7] Ashifa, K. M. (2021b). Health status of primitive tribal women in India. Journal of Cardiovascular Disease Research, 12(5), 772.

[8] Ashifa, K. M. (2022). A situation analysis of the social well-being of elderly during the COVID-19 pandemic. International Journal of Health Sciences, 6(3), 10156–10163.

[9] Ashifa, K. M., & Ramya, P. (2019). Health afflictions and quality of work life among women working in fireworks industry. International Journal of Engineering and Advanced Technology, 8(6S3), 1723–1725.

[10] Basha, R., Pathak, P., Sudha, M., Soumya, K. V., & Arockia Venice, J. (2025). Optimization of quantum dilated convolutional neural networks: Image recognition with quantum computing. Internet Technology Letters, 8(3), e70027.

[11] Devi, M., Manokaran, D., Sehgal, R. K., Shariff, S. A., & Vettriselvan, R. (2025). Precision medicine, personalized treatment, and network-driven innovations. In AI for large scale communication networks (pp. 303–322). IGI Global.

[12] Elkin, N., Mohammed, A. K., Kılınçel, Ş., Soydan, A. M., Tanrıver, S. Ç., Çelik, Ş., & Ranganathan, M. (2025). Mental health literacy and happiness among university students. Frontiers in Psychiatry, 16, 1541316.



DOI: 10.30726/ijlca/v13.i2.2026.132008

[13] Gayathri, R. K., Vettriselvan, R., Rajesh, D., Balakrishnan, R., Kumar, R., & Kavitha, J. (2025a). Striking a balance: Mental health challenges and work-life integration among women faculty in Indian B-Schools. Texila International Journal of Public Health, 13(2).

[14] Gayathri, R. K., Vettriselvan, R., Rajesh, D., Balakrishnan, R., Kumar, R., & Kavitha, J. (2025b). Strategic role of human resource management in enhancing occupational health and safety practices. Texila International Journal of Public Health, 13(2).

[15] Jenifer, R. D., Vettriselvan, R., Saxena, D., Velmurugan, P. R., & Balakrishnan, A. (2025). Green marketing in healthcare advertising: A global perspective. In AI impacts on branded entertainment and advertising (pp. 303–326). IGI Global.

[16] Kariveliparambil, A., Rasi, R. A., Ahmad, M. S., Öztaş, N., & Ayan, F. S. (2026a). Evolving social capital in indigenous communities. Journal of Social Service Research, 52(1), 147–166.

[17] Kariveliparambil, A., R A, R., Ahmad, M. S., Ramesh, S., & Kuriakose, A. (2026b). Invisible burdens of platform work. International Journal of Qualitative Studies on Health and Well-Being, 21(1).

[18] Kombo, D. K., & Tromp, D. L. A. (2014). Proposal and thesis writing: An introduction. Paulines Publications Africa.

[19] Meena, G., Vettriselvan, R., Rajesh, D., & Velmurugan, P. R. (2025). Diversity and inclusion: Harnessing the power of inclusivity for business success. In Security and strategy models for key-solving institutional frameworks (pp. 203–234). IGI Global Scientific Publishing.

[20] Mohanbabu, S., & Vettriselvan, R. (2025a). Focusing supply chain and container terminal challenges. International Journal of Procurement Management, 24(1), 92–114.

[21] A. S. Aneeshkumar, Sandramol M Kamal (2024). A literature study on Cybercrime in social media using Genetic Algorithm based Datamining Techniques, Journal of Electrical Systems, 20(3), pp. 4382-4390

[22] Mohanbabu, S., & Vettriselvan, R. (2025b). Will machine learning resolve the issues in container management. International Journal of Process Management and Benchmarking, 20(4), 559–575.

[23] Orodho, J. A., & Kombo, D. K. (2012). Research methods. Kenyatta University Press.

[24] Rajeswari, M., Rohini, V., Sathya Aarthi, R., Rameshkumaar, V. P., & Arul Krishnan, S. (2026). Blockchain 2.0 for secure, transparent, and autonomous logistics systems. In R. Vettriselvan & N. Suresh (Eds.), Intelligent motion control for human-centered systems (pp. 233–258). IGI Global Scientific Publishing.

[25] Ranganathan, M., Jacob, A., Ashifa, K. M., Kumar, G. J., Anthony, M., Vijay, M., & Kumari, R. B. (2024). An investigation of the effects of chronic stress on attention in parents of children with neurodevelopmental disorders. Universal Journal of Public Health, 12(1), 37–50.

[26] Rasi, R. A., & Ashifa, K. M. (2019). Role of community-based programmes for active ageing. Indian Journal of Public Health Research & Development, 10(12).

[27] Shanthi, H. J., Gokulakrishnan, A., Sharma, S., Deepika, R., & Swadhi, R. (2025). Leveraging artificial intelligence for enhancing urban health. In Nexus of AI, climatology, and urbanism for smart cities (pp. 275–306). IGI Global.

[28] Swadhi, R., Gayathri, K., Suresh, N. V., Catherine, S., & Velmurugan, P. R. (2025a). Leveraging machine learning for enhanced patient engagement and outcomes. In Impact of digital transformation on business growth and performance (pp. 313–340). IGI Global Scientific Publishing.

[29] Swadhi, R., Velmurugan, P. R., Gayathri, K., & Catherine, S. (2025b). Evolving critical themes in advanced human resource management. In Critical aspects in advanced human resource management (pp. 75–102). IGI Global Scientific Publishing.

[30] Vasantha, S., Swadhi, R., Gayathri, K., Selvalakshmi, V., & UmaDevi, A. (2025). Fostering personalized learning and achieving equity in education. In Transforming education with AI-powered personalized learning (pp. 201–236). IGI Global Scientific Publishing.

[31] Venice, J. A., Arivazhagan, D., Suman, N., Shanthi, H. J., & Swadhi, R. (2025a). Recommendation systems and content personalization. In AI for large scale communication networks (pp. 323–348). IGI Global Scientific Publishing.

[32] Venice, J. A., Vettriselvan, R., Jain, S., Madusudanan, K., & Aarthy, C. C. J. (2025b). Performance evaluation and metrics in blockchain powered AI/ML. In Transforming education with AI-powered personalized learning (pp. 143–178). IGI Global Scientific Publishing.

[33] Venice, J. A., Vettriselvan, R., Rajesh, D., Suresh, N. V., & Abirami, P. (2025c). Enabling personalized learning and adaptive systems through strategic management. In Bridging academia and industry through cloud integration in education (pp. 49–72). IGI Global Scientific Publishing.

[34] Venice, J. A., Vettriselvan, R., Rajesh, D., Xavier, P., & Shanthi, H. J. (2025d). Optimizing performance metrics in blockchain-enabled AI/ML data analytics. In Enhancing automated decision-making through AI (pp. 97–122). IGI Global.

[35] Venice, J. A., Sripathi, S. K., & Moonga, B. (2025e). Social deviance and the influence of internet exposure. ASET Journal of Management Science, 4(SI-1).

[36] Venice, J. A. A., Jio, W., Kant, S., Sharda, S., & Mittal, S. (2025f). Ethical leadership effect on the regulation of AI in cyber security. In Ethical challenges of AI and warfare (pp. 133–152). IGI Global Scientific Publishing.

[37] Venice, J. A. A., Muthuraman, M., Kant, S., & Mittal, S. (2026). Community engagement effect on school leadership through digital volunteerism. In Strengthening community engagement and school leadership through digital volunteerism (pp. 85–114). IGI Global Scientific Publishing.

[38] Vettriselvan, R. (2025). Harnessing innovation and digital marketing in the era of industry 5.0. In The future of small business in industry 5.0 (pp. 163–186). IGI Global.

[39] Vettriselvan, R., & Anto, M. R. (2018). Pathetic health status and working condition of Zambian women. Indian Journal of Public Health Research & Development, 9(9), 259–264.

[40] Vettriselvan, R., & Rajan FSA, A. J. (2019). Occupational health issues faced by women in spinners. Indian Journal of Public Health Research & Development, 10(1).

[41] Vettriselvan, R., Deepan, A., Jaiswani, G., Balakrishnan, A., & Sakthivel, R. (2025a). Health consequences of early marriage. In Social, political, and health implications of early marriage (pp. 189–212). IGI Global.

[42] Vettriselvan, R., Velmurugan, P. R., Varshney, K. R., EP, J., & Deepika, R. (2025b). Health impacts of smartphone and internet addictions across age groups. In Impacts of digital technologies across generations (pp. 187–210). IGI Global.

[43] Vettriselvan, R., Velmurugan, P. R., Suresh, N. V., & Catherine, S. (2025c). Strategies, best practices, and pitfalls in the era of digital transformation. In Impact of digital transformation on business growth and performance (pp. 67–98). IGI Global Scientific Publishing.

[44] Vettriselvan, R., Selvi, K., Kumar, A. S., Ranjani, R. D., & Varshney, K. R. (2025d). Ranking methodologies: Criteria and controversies in global higher education. In Global university ranking systems (pp. 109–140). IGI Global Scientific Publishing.

[45] Vettriselvan, R., Gokuldas, P. G., & Sambamoorthy, N. (2025e). Designing language materials to motivate, engage, and empower learners. In Exploring the psychology of language materials development (pp. 279–302). IGI Global Scientific Publishing.

[46] Vettriselvan, R., Ramya, R., Selvalakshmi, V., Jyothi, P., & Velmurugan, P. R. (2026a). Empowering patients through knowledge: Educational strategies in rehabilitation. In Holistic approaches to health recovery (pp. 263–290). IGI Global Scientific Publishing.

[47] Vettriselvan, R., Velmurugan, P. R., Savariapitchai, M., & Swadhi, R. (2026b). AI and international volunteering. In Impacts of AI on international volunteering (pp. 1–24). IGI Global Scientific Publishing.



**DOI: 10.30726/ijlca/v13.i2.2026.132008**

[48] Vijayalakshmi, M., Subramani, A. K., Vettriselvan, R., Catherin, T. C., & Deepika, R. (2025a). Sustainability and responsibility in the digital era. In Digital citizenship and building a responsible online presence (pp. 285–306). IGI Global.

[49] Vijayalakshmi, M., Subramani, A. K., Vettriselvan, R., Velmurugan, P. R., & Hasine, J. (2025b). Strategic collaborations in medical innovation and AI-driven globalization. In Navigating strategic partnerships for sustainable startup growth (pp. 85–110). IGI Global.

[50] Vinodh, N., Subramani, A. K., & Vettriselvan, R. (2026a). Navigating ethics, society, and governance in the digital age. In Ethics, justice, and governance in the age of AI and digital societies (pp. 1–26). IGI Global Scientific Publishing.

[51] Vinodh, N., Subramani, A. K., & Vettriselvan, R. (2026b). Transforming the future of management and medical education. In AI education strategies for future-proofing curriculum design (pp. 459–476). IGI Global Scientific Publishing.

[52] Zahoor, H., Mustafa, N., Ashifa, K. M., Safaei, M., & El Gamil, R. (2025). Unlocking resilience: Emotional intelligence and self-leadership shape stress perception among health students. International Journal of Innovation and Learning, 38(4), 395–419.



**DOI: 10.30726/ijlca/v13.i2.2026.132008**