Cyber Security Experts Association of Nigeria (CSEAN)
Society for Multidisciplinary & Advanced Research Techniques (SMART)
West Midlands Open University
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
ICT University Foundations USA
Academic Innovations City University Foundations

Proceedings of the Cyber Secure Nigeria Conference – 2024

AI-Driven Strategies for Enhancing Human Cybersecurity Awareness in Nigeria.

Jonathan Ayodele
BitScape Technologies
School of Computer and Informatics, Cardiff University, Cardiff, United Kingdom.
E-mail; ayodelejona@gmail.com
Phone: +447548916207

ABSTRACT

As Nigeria experiences rapid digital growth, its cybersecurity challenges continue to escalate, driven by an expanding internet user base and the increasing sophistication of cyber threats targeting organisations with human vulnerabilities being a key entry point. Traditional cybersecurity awareness programs have struggled to keep pace with evolving threats, necessitating the adoption of Artificial Intelligence (AI)-driven strategies to enhance human cybersecurity awareness. This paper explores AI-driven strategies for enhancing human cybersecurity awareness in Nigeria, focusing on the unique socio-economic and cultural challenges that influence the effectiveness of traditional awareness programs. AI offers transformative solutions by enabling personalised training, real-time threat detection, and predictive analytics, making it a critical tool for addressing Nigeria's evolving cyber threat landscape. However, barriers such as inadequate infrastructure, limited technical expertise, and data limitations hinder the full adoption of AI in cybersecurity. The paper concludes with recommendations for implementing AI-driven cybersecurity awareness programs tailored to Nigeria's needs, including enhanced collaboration between government, educational institutions, and the private sector to foster a cybersecurity culture. By leveraging AI, Nigeria can significantly bolster its defences, ensuring a secure digital future for its growing online population.

Keywords: Cybersecurity, Artificial Intelligence, Strategies, Human-AI Collaboration, Nigeria,

Proceedings Citation Format
Jonathan Ayodele (2024): AI-Driven Strategies for Enhancing Human Cybersecurity Awareness in Nigeria. Proceedings of the Cyber Secure Nigeria Conference. Proceedings of the Cyber Secure Nigeria Conference held at The Ballroom Center, Central Business District, Federal Capital Territory, Abuja, Nigeria - 25th - 26th September, 2024. Pp 141-150. https://cybersecurenigeria.org/conference-proceedings/volume-1-2024/ dx.doi.org/10.22624/AIMS/CSEAN-SMART2024P13

1. INTRODUCTION

As digital technologies continue to reshape economies and societies, cybersecurity has emerged as a critical issue globally, and Nigeria is no exception. Nigeria, with a population of over 200 million people (Ihugba, 2020), has one of the youngest and most tech-savvy populations in the world. By the start of 2024, Nigeria had an impressive 103 million internet users, reflecting a significant increase from 83 million in 2022, which at the time constituted approximately 39% of the population (Statista, 2024) With an expected 48% growth in the number of users by 2027, the country is poised to become a major player in the digital economy. (Kemp, 2024).

Despite these advances, Nigeria faces substantial challenges in cybersecurity. The internet penetration rate in the country currently stands at about 55%, with roughly 123 million active internet users (Kemp, 2024). This growing digital footprint, while essential for economic and social development, also exposes the country to a higher risk of cyber threats. As more Nigerians engage with digital platforms—whether for financial transactions, e-commerce, or social interactions—the need for robust cybersecurity frameworks becomes increasingly urgent. With its vast internet audience, Nigeria is uniquely vulnerable to cybercrimes, which range from sophisticated forms of digital fraud and ransomware. The rapid digitisation of sectors such as banking, telecommunications, and government services has compounded this problem, making individuals, organisations, and governments more vulnerable to cyberattacks, particularly those that exploit human errors, making cybersecurity awareness and resilience a national priority.

Despite increased investments in technology to protect digital assets, human vulnerabilities remain one of the primary avenues through which cybercriminals successfully execute attacks (Ayyad et al., 2024). This highlights the importance of enhancing cybersecurity awareness to mitigate these risks. Traditional cybersecurity awareness programs, which rely heavily on manual training and generic content, have often fallen short in keeping up with the ever-evolving nature of cyber threats (Adeboye Popoola et al., 2024) They typically fail to engage users effectively or provide the personalised learning necessary to foster behavioural changes (Brehmer et al., 2024). As a result, many individuals and organisations remain unprepared to defend against common attack vectors, such as phishing scams, ransomware, and social engineering tactics.

Artificial Intelligence (AI) presents a promising solution to this challenge. By leveraging AI, organisations can create more dynamic, adaptive, and personalised cybersecurity awareness programs that address specific user vulnerabilities and learning styles. AI's ability to analyse large data sets, predict human behaviour, and offer real-time feedback makes it an ideal tool for delivering targeted awareness interventions. As Nigeria seeks to strengthen its cybersecurity posture, adopting AI-driven strategies for human cybersecurity awareness becomes an essential part of the solution. This paper explores how AI can be effectively integrated into cybersecurity awareness programs to enhance the overall security culture in Nigeria. It examines the potential of AI to transform traditional awareness efforts, assesses current barriers to its adoption, and provides recommendations for implementing AI-driven solutions tailored to Nigeria's unique cybersecurity landscape.

1.1 Background on cybersecurity in Nigeria

Nigeria has experienced significant challenges in cybersecurity, driven largely by the rapid adoption of digital technologies across its public and private sectors. As the largest economy in Africa and with a growing digital infrastructure, Nigeria faces increased threats from cybercrime and cyberattacks (A. Ajayi, 2024). The country has implemented various cybersecurity policies, but challenges such as weak enforcement mechanisms, insufficient infrastructure, and inadequate public awareness persist (Avosetinyen et al., 2024). Cybersecurity awareness in Nigeria is still in its infancy, with a critical need for capacity-building initiatives focusing on designing and implementing campaigns to educate citizens on cyber risks (Bada et al., 2019). This gap in awareness has been identified as a contributing factor to the proliferation of cybercrime across the country.

The Nigerian government has enacted legislation, such as the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015, to combat cybercrime and regulate online activities. This law addresses offences like fraud, identity theft, and unauthorised data access, while also establishing frameworks to prosecute offenders (Izevbuwa & Rita, 2022). In addition to this legislation, Nigeria has implemented structures to support cybersecurity, including the establishment of a national Computer Emergency Response Team (CERT) and several sectoral Computer Security Incident Response Teams (CSIRTs), reflecting efforts to improve coordination and incident response (Ikuero, 2022). Despite these efforts, issues such as the administration of cybersecurity levies and the proper enforcement of cybercrime laws remain contentious (U. M. N. Nwoke & Theophilus, 2024).

Cyberattacks, such as Distributed Denial of Service (DDoS), have also increasingly targeted Nigeria's critical national information infrastructure, posing threats to economic stability and national security (Zwingina et al., 2024). Studies have also highlighted that Nigerian users demonstrate a higher level of cybersecurity awareness compared to some other nations, which is crucial for bolstering digital defences (Nnamdi et al., 2023). However, the effectiveness of these measures is often limited by the lack of a comprehensive cybersecurity culture. Efforts to foster such a culture include promoting cybersecurity awareness, education, and the development of relevant policies, particularly in sectors like online banking, which remains vulnerable to cyber threats (Garba et al., 2023a).

1.2. Current Cybersecurity Challenges in Nigeria

Nigeria faces numerous cybersecurity challenges, driven by a mix of socio-economic factors and an evolving cyber threat landscape. Nigeria's socio-economic conditions, such as poverty, exacerbate the problem, making cybersecurity a matter of national security. Cybercriminals exploit vulnerable populations, targeting individuals and businesses, often using social media platforms as a tool for fraudulent activities (Akinyetun, 2021) (D. Oni et al., 2023). The COVID-19 pandemic exacerbated these challenges, leading to a spike in cybercrimes as more individuals relied on online platforms for work and social interaction. Poor cybersecurity measures during this period led to significant vulnerabilities, which have only recently begun to be addressed through updated cybersecurity strategies and improved awareness (Nainna et al., 2024).

Additionally, political instability and corruption contribute to a culture of impunity, where security threats, including cybercrime, policy enforcement, are not adequately addressed by law enforcement or governmental authorities (Unaji, 2013). The evolution of cybercrime in Nigeria from traditional "419" scams to sophisticated malware attacks highlights the increasing complexity of the threat landscape. Nigerian cybercriminals are becoming more adept at using advanced techniques, posing a global cybersecurity threat (Hinchliffe, 2017). Addressing these challenges requires not only legislative reform and better coordination among cybersecurity bodies but also a holistic approach that tackles the socio-economic drivers of cybercrime, promotes public awareness, and implements robust cybersecurity frameworks across various sectors, including education and finance (Odumesi, 2014).

2. AI-DRIVEN CYBERSECURITY AWARENESS STRATEGIES

The increasing sophistication of cyber threats in Nigeria calls for equally advanced solutions. Artificial Intelligence (AI) has emerged as a powerful tool in enhancing cybersecurity by enabling faster detection, prevention, and response to cyberattacks. AI-driven cybersecurity strategies can be particularly effective in addressing the challenges posed by Nigeria's rapidly growing digital landscape. By leveraging these techniques, AI systems can detect and analyse patterns in large datasets, enabling the identification of emerging cyber threats and the development of strategies to prevent potential breaches before they occur (Alionsi, 2023). Below are some key AI-driven strategies to enhance cybersecurity awareness:

Personalised Cybersecurity Training Programs

One of the major reasons for cybersecurity breaches is a lack of awareness among users. AI can be utilised to personalise cybersecurity training and awareness programs for different categories of internet users. Machine learning algorithms can assess user behaviour and knowledge gaps, tailoring training modules to the needs of each user. For instance, employees in the banking sector may require more intensive training on phishing, while users in the healthcare sector may focus on protecting patient data. These AI-driven platforms enable users to comprehend complex cybersecurity rules and implement them effectively, thus improving the overall cybersecurity awareness among individuals and organisations (Jawhar et al., 2024).

Personalised Cybersecurity Awareness Programs

AI-driven cybersecurity solutions empower users by enhancing their awareness and response capabilities through personalised security measures. These solutions can analyse user behaviour and system vulnerabilities, providing tailored recommendations for mitigating risks. The implementation of these AI strategies leads to improved overall cybersecurity posture, particularly for businesses and individuals in Nigeria (Ofoegbu et al., 2023).

Predictive Analytics for Proactive Cybersecurity

AI-driven predictive analytics allows organisations to stay ahead of potential cyber threats by analysing trends and forecasting future risks. By utilising historical data, AI can predict when and how cyberattacks are likely to occur, providing organisations with the opportunity to prepare in advance. Predictive models can also identify vulnerable points in a system, allowing organisations to patch weaknesses before they are exploited by attackers.

This proactive approach is crucial for Nigeria's rapidly expanding digital infrastructure, which will likely face more sophisticated cyberattacks in the future. Predictive analytics can also help prioritise resources, ensuring that critical systems are fortified against the most probable attacks (Ayorinde Dada et al., 2024).

AI-Enhanced Public Awareness Campaigns

In addition to internal organisational strategies, AI can be leveraged in public awareness campaigns aimed at educating Nigeria's broader population about cybersecurity (Abdelhamid et al., 2023). Chatbots, for instance, can provide users with real-time information on how to protect themselves online, answer frequently asked questions, and guide users through safe internet practices. Furthermore, AI can analyse the effectiveness of cybersecurity awareness campaigns, allowing for the optimisation of content delivery. AI-powered tools can determine which demographics are most at risk and tailor campaigns to address specific vulnerabilities (Chaudhary & Gkioulos, 2023).

Combating Misinformation and Fake News

Misinformation and fake news, often spread through social media, can fuel cyberattacks, particularly through phishing schemes and fraudulent campaigns. AI-driven systems can scan social media platforms for misinformation, identify fake accounts, and track the spread of false information. These systems can automatically flag suspicious content, reducing the chances of users falling victim to cyber scams. For a country like Nigeria, where mobile and social media usage is high, AI tools can play a critical role in reducing the spread of harmful misinformation that could compromise cybersecurity.

3. BARRIERS TO ADOPTING AI FOR CYBERSECURITY AWARENESS IN NIGERIA

Despite the potential benefits of integrating AI into cybersecurity awareness strategies, Nigeria faces several barriers that hinder the full adoption and implementation of AI in this field. These barriers span across technical, economic, and infrastructural challenges, limiting the ability to leverage AI to its fullest potential. Some of the key barriers include: One major obstacle is the lack of adequate infrastructure, particularly in rural areas where internet penetration remains low (Nibigira et al., 2024), which limits the effectiveness of AI-driven systems. Nigeria's digital divide, especially in terms of internet access and technological resources, stifles the widespread use of AI in combating cybercrime. Additionally, the country's under-exploitation of available ICT tools, such as security gadgets and AI technologies, has led to insufficient protection against cyber threats (Ugwueze et al., 2016).

Another major challenge to the adoption of AI for cybersecurity awareness in Nigeria is the lack of technical expertise. AI systems require a specialised skill set to develop, maintain, and integrate effectively into existing cybersecurity frameworks. Nigeria's labour market still struggles with a shortage of professionals equipped with the necessary skills in AI, machine learning, and cybersecurity. As a result, organisations find it difficult to deploy advanced AI-driven cybersecurity solutions, which hinders progress in building comprehensive awareness campaigns (Ogunleye, 2021). Similarly, AI relies heavily on large datasets to function effectively, particularly in cybersecurity, where it must analyse patterns and detect anomalies. However, in Nigeria, there is a lack of structured and accessible data necessary for training AI models.

This scarcity of data limits the capacity of AI tools to learn from existing threats and respond to new ones. In addition, concerns over data privacy and protection also hinder the collection and sharing of data, which is crucial for effective AI-driven cybersecurity awareness (Mark, 2024). The legal and regulatory landscape also presents challenges to the adoption of AI for cybersecurity. While Nigeria has enacted cybercrime legislation such as the Cybercrimes (Prohibition, Prevention, etc.) Act, the country still faces difficulties in enforcing these laws effectively. The lack of robust legal frameworks and clear guidelines for AI use in cybersecurity creates uncertainty for businesses and institutions considering AI adoption (S. Oni et al., 2019). The absence of clear and comprehensive policies governing AI in Nigeria further hinders its adoption in cybersecurity. Furthermore, the lack of government incentives or support for AI adoption discourages widespread implementation across sectors (Uba, 2023).

Cultural Considerations in Cybersecurity Awareness

In Nigeria, cybersecurity awareness efforts face unique challenges shaped by the country's diverse cultural, social, and economic landscape. As a nation with over 250 ethnic groups, varying levels of digital literacy, and diverse socioeconomic backgrounds, promoting cybersecurity awareness must account for these cultural dynamics to be effective. Cultural beliefs, attitudes toward technology, and the level of trust in digital systems can all influence how individuals and communities respond to cybersecurity education and practices. These elements shape how individuals perceive and respond to cybersecurity threats, particularly in sectors like online banking, where cybersecurity practices must be aligned with users' cultural expectations (J. Garba et al., 2023b).

One of the main cultural considerations is the level of digital literacy, which varies significantly between urban and rural populations in Nigeria. While urban centres like Lagos and Abuja are more digitally advanced, many rural areas lag in internet penetration and understanding of basic cybersecurity principles. This disparity is exacerbated by socioeconomic factors, where individuals with lower income levels often prioritise access to basic needs over investing in secure digital practices (Chikwendu & Oli, 2023).

Cultural attitudes towards trust and authority play a pivotal role in shaping cybersecurity behaviours. For example, many Nigerians may be more likely to trust information from personal networks and community leaders than from formal institutions. This cultural dynamic affects how cybersecurity awareness campaigns should be structured, as localised and community-driven approaches may be more effective than top-down government-led initiatives (C. N. Nwoke et al., 2021). Therefore, cybersecurity awareness campaigns must engage community leaders and influencers to disseminate accurate information and foster trust in digital systems (J. Garba et al., 2023c).

Nigeria is a multilingual country with over 500 languages spoken. Cybersecurity awareness campaigns must consider language diversity to reach a wider audience. English is commonly used in formal settings and for digital communication, but for cybersecurity awareness to be effective, local languages should be integrated into training materials and campaigns, particularly in rural areas where English proficiency may be limited (Adejumo, 2024). Awareness programs must consider local languages and communication styles to ensure that cybersecurity messages are accessible to diverse audiences across the country (Adelola et al., 2015).

4. RECOMMENDATIONS FOR IMPLEMENTING AI-DRIVEN AWARENESS PROGRAMS IN NIGERIA

To effectively enhance cybersecurity awareness in Nigeria through AI-driven solutions, several key recommendations can be implemented. One of the primary steps is the establishment of a national cybersecurity awareness program, driven by AI technologies. The urgent need for such a program has been highlighted, particularly in the context of addressing Nigeria's current lack of government-led initiatives. This program would help foster a cybersecurity culture across all levels of society, ensuring that citizens, businesses, and policymakers are educated about cyber threats and the role of AI in mitigating them.

Successful implementation of AI-driven cybersecurity awareness programs requires collaboration between the Nigerian government, the private sector, and educational institutions. The government should spearhead national initiatives to ensure the wide-scale adoption of AI in cybersecurity training. By incorporating AI tools into schools and universities, students can develop cybersecurity skills early on, which will benefit the broader population as they enter the workforce (A. Garba et al., 2020).

For AI-driven awareness programs to be impactful, they must be integrated with Nigeria's existing national cybersecurity policies and strategies. AI can enhance current efforts by offering real-time threat detection, monitoring, and reporting mechanisms. Government agencies responsible for cybersecurity, such as the National Information Technology Development Agency (NITDA), should collaborate with AI vendors to ensure that AI tools align with national security objectives and regulatory requirements (Femi-Oyewole, 2024).

5. CONCLUSION

As Nigeria continues its rapid digital transformation, the importance of strengthening cybersecurity awareness cannot be overstated. The country's large, youthful population and growing internet penetration present both opportunities and challenges. Cyber threats are becoming increasingly sophisticated, and traditional methods of addressing them are no longer sufficient. AI-driven strategies offer a promising solution, providing advanced tools for detecting threats, automating responses, and educating users on best cybersecurity practices.
In conclusion, AI has the potential to revolutionise cybersecurity awareness in Nigeria, offering scalable, efficient, and personalised solutions. By leveraging AI's capabilities and addressing existing barriers, Nigeria can safeguard its digital future, fostering trust and resilience in its rapidly expanding online ecosystem.

REFERENCES

A. Ajayi, O. (2024). Internet Technologies and Cybersecurity Law in Nigeria. In Malthouse Press. https://muse.jhu.edu/pub/400/monograph/book/126489

Abdelhamid, S., Mallari, T., & Aly, M. (2023). Cybersecurity Awareness, Education, and Workplace Training Using Socially Enabled Intelligent Chatbots. Lecture Notes in Networks and Systems, 767 LNNS, 3–16. https://doi.org/10.1007/978-3-031-41637-8_1/FIGURES/8

Adeboye Popoola, O., Oladipo Akinsanya, M., Nzeako, G., Chukwurah, E. G., David Okeke, C.,& Author, C. (2024). Exploring theoretical constructs of cybersecurity awareness and training programs: comparative analysis of African and U.S. Initiatives. International Journal of Applied Research in Social Sciences, 6(5), 819–827. https://doi.org/10.51594/IJARSS.V6I5.1104

Adejumo, D. A. (2024). Digitalisation and Country Profile: Towards a Framework for the promotion of Nigeria National Image. Research Forum of the University of Aveiro - UA Editora – Universidade de Aveiro, 16–19.

Adelola, T., Dawson, R., & Batmaz, F. (2015). The urgent need for an enforced awareness programme to create internet security awareness in nigeria. Proceedings of the 17th International Conference on Information Integration and Web-Based Applications & Services, 1–7. https://doi.org/10.1145/2837185.2837237

Akinyetun, T. S. (2021). Poverty, Cybercrime and National Security in Nigeria. Journal of Contemporary Sociological Issues, 1(2), 86. https://doi.org/10.19184/csi.v1i2.24188

Alionsi, D. D. D. (2023). AI-driven cybersecurity: Utilizing machine learning and deep learning techniques for real-time threat detection, analysis, and mitigation in complex IT networks. Advances in Engineering Innovation, 3(1), None-None. https://doi.org/10.54254/2977-3903/3/2023036

Avosetinyen, M. S., Sanni, M. O., Erubami, H. P., & Akinyetun, T. S. (2024). COVID-19, Cybercrime Proliferation, and National Security in Nigeria: Evidence from Lagos State Youths. Commonwealth Youth and Development, 22 pages-22 pages. https://doi.org/10.25159/2663-6549/16212

Ayorinde Dada, M., Sunday Oliha, J., Tega Majemite, M., Obaigbena, A., Winston Biu, P., & Author, C. (2024). A REVIEW OF PREDICTIVE ANALYTICS IN THE EXPLORATION AND MANAGEMENT OF U.S. GEOLOGICAL RESOURCES. Engineering Science & Technology Journal, 5(2), 313–337. https://doi.org/10.51594/ESTJ.V5I2.763

Ayyad, W. R., Al-Haija, Q. A., & Al-Masri, H. M. K. (2024). Human Factors in Cybersecurity. In https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/979-8-3693-3451-5.ch011 (pp. 235–256). IGI Global. https://doi.org/10.4018/979-8-3693-3451-5.ch011

Bada, M., von Solms, B., & Agrafiotis, I. (2019). Reviewing National Cybersecurity Awareness in Africa: An Empirical Study. https://doi.org/10.17863/CAM.40856

Brehmer, M., Steinherr, V., & Stöckl, R. (2024). Toward A Higher Resilience Against Cyberattacks. Datenschutz Und Datensicherheit - DuD 2024 48:6, 48(6), 352–357. https://doi.org/10.1007/S11623-024-1923-0

Chaudhary, S., & Gkioulos, V. (2023). Building a Cybersecurity Awareness Program: Present and Prospective Aspects. Communications in Computer and Information Science, 1807 CCIS, 149–160. https://doi.org/10.1007/978-3-031-36096-1_10/FIGURES/1

Chikwendu, S. C., & Oli, N. P. (2023). Human Factors influencing Compliance to Cyber Security Practices by Employees of Public Universities in Southeast Nigeria. International Journal of Information Security, Privacy and Digital Forensics, 7(1). https://www.nigerianjournalsonline.com/index.php/NCS/article/view/3915

Femi-Oyewole, F. (2024). Nigeria's Cybersecurity Challenge: Four Steps To Curb Cybercrime. Forbes Technology Council. https://www.forbes.com/councils/forbestechcouncil/2024/02/06/nigerias-cybersecurity-challenge-four-steps-to-curb-cybercrime/

Garba, A., Siraj, M. M., Othman, S. H., & Musa, M. A. (2020). A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach. International Journal on Emerging Technologies, 41–49. https://www.researchtrend.net/ijet/pdf/A%20Study%20on%20Cybersecurity%20Awareness%20Among%20Students%20In%20Yobe%20State%20University%20Nigeria%20A%20Quantitative%20Approach%20%20Adamu%20A6.pdf

Garba, J., Kaur, J., & Ibrahim, E. N. M. (2023a). Design of a conceptual framework for cybersecurity culture amongst online banking users in Nigeria. Nigerian Journal of Technology, 42(3), 399–405. https://doi.org/10.4314/njt.v42i3.13

Garba, J., Kaur, J., & Ibrahim, E. N. M. (2023b). Design of a conceptual framework for cybersecurity culture amongst online banking users in Nigeria. Nigerian Journal of Technology, 42(3), 399–405. https://doi.org/10.4314/njt.v42i3.13

Garba, J., Kaur, J., & Ibrahim, E. N. M. (2023c). Design of a conceptual framework for cybersecurity culture amongst online banking users in Nigeria. Nigerian Journal of Technology, 42(3), 399–405. https://doi.org/10.4314/njt.v42i3.13

Hinchliffe, A. (2017). Nigerian princes to kings of malware: the next evolution in Nigerian cybercrime. Computer Fraud & Security, 2017(5), 5–9. https://doi.org/10.1016/S1361-3723(17)30040-4

Ikuero, F. E. (2022). Preliminary review of cybersecurity coordination in Nigeria. Nigerian Journal of Technology, 41(3), 521–526. https://doi.org/10.4314/njt.v41i3.11

Izevbuwa, O. G., & Rita, A. N. (2022). Combating the Menace of Cybercrime in Nigeria: A Review of the Cybercrime (Prohibition, Prevention etc) Act 2015 and Other Legislations. Journal of Law, Policy and Globalization. https://doi.org/10.7176/JLPG/119-01

Jawhar, S., Miller, J., & Bitar, Z. (2024). AI-Driven Customized Cyber Security Training and Awareness. 2024 IEEE 3rd International Conference on AI in Cybersecurity, ICAIC 2024. https://doi.org/10.1109/ICAIC60265.2024.10433829

Kemp, S. (2024, February 23). Digital 2024: Nigeria — DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2024-nigeria

Mark, D. (2024). Impact of Artificial Intelligence on Cybersecurity in Nigeria. American Journal of Computer and Engineering.

Nainna, M. A., Bass, J., & Speakman, L. (2024). Cyber Threat Intelligence Sharing in Nigeria. Communications of the IIMA, 22(1), 1. https://doi.org/10.58729/1941-6687.1450

Nibigira, N., Havyarimana, V., & Xiao, Z. (2024). Artificial Intelligence Adoption for Cybersecurity in Africa. Journal of Information Security, 15(02), 134–147. https://doi.org/10.4236/jis.2024.152009

Nnamdi, I., Kingsley Chukwuemeka, U., Peace Nkirika, U., & Obiora, I. (2023). ANALYSIS OF CYBER-SECURITY CONSCIOUSNESS AND EDUCATION STRATEGY IN NIGERIA. International Research Journal of Modernization in Engineering Technology and Science. https://doi.org/10.56726/IRJMETS44025

Nwoke, C. N., Nzeakor, O. F., Nwoha, N. G., Ugwu, O., Uba-Uzoagwa, O. P., & Ikenegbu, T. G. (2021). Determinants of Cybercrime Awareness Among Internet users in Nigeria. International Journal of Humanities and Social Science, Volume 8(5), 14–22. https://doi.org/10.14445/23942703/IJHSS-V8I5P103

Nwoke, U. M. N., & Theophilus, W. N. (2024). An Assessment of the Legal Validity of the Cybersecurity Levy in Nigeria. Multidisciplinary Journal Of Law, Education And Humanities, 1(2). https://nigerianjournalsonline.com/index.php/MJLEH/article/view/5226

Odumesi, J. O. (2014). A socio-technological analysis of cybercrime and cybersecurity in Nigeria. International Journal of Sociology and Anthropology, 6(3), 116–125. https://doi.org/10.5897/IJSA2013.0510

Ofoegbu, K. D. O., Osundare, O. S., Ike, C. S., Fakeyede, O. G., & Ige, A. B. (2023). Empowering users through AI-driven cybersecurity solutions: enhancing awareness and response capabilities. Engineering Science & Technology Journal, 4(6), 707–727. https://doi.org/10.51594/ESTJ.V4I6.1528

Ogunleye, I. (2021). Artificial Intelligence for Economic Development in Nigeria. https://citrispolicylab.org/wp-content/uploads/2021/12/Artificial-Intelligence-for-Economic-Development-in-Nigeria_Ifejesu-Ogunleye.pdf

Oni, D., Arshad, E., & Pham, B. N. (2023). Cybercrime On Social Media In Nigeria: Trends, Scams, Vulnerabilities and Prevention. Advances in Multidisciplinary and Scientific Research Journal Publication, 2(1), 143–150. https://doi.org/10.22624/AIMS/CSEAN-SMART2023P17

Oni, S., Araife Berepubo, K., Oni, A. A., & Joshua, S. (2019). E-Government and the Challenge of Cybercrime in Nigeria. 2019 Sixth International Conference on EDemocracy & EGovernment (ICEDEG), 137–142. https://doi.org/10.1109/ICEDEG.2019.8734329

Ihugba, O. A. (2020). Population growth in Nigeria: implications for primary school enrolment. Journal of School of Arts and Social Sciences JOSASS. https://www.researchgate.net/profile/Okezie-Ihugba/publication/373137008_Population_growth_in_Nigeria_implications_for_primary_school_enrolment/links/64db88e578e40b48bd4c90eb/Population-growth-in-Nigeria-implications-for-primary-school-enrolment.pdf#page=242

Statista. (2024). Nigeria internet user penetration 2027 | Statista. https://www.statista.com/statistics/484918/internet-user-reach-nigeria/

Uba, J. (2023). Artificial Intelligence (AI) Application In Cybersecurity: A Synergistic Approach To Safeguarding The Digital Realm . https://www.mondaq.com/nigeria/new-technology/1353056/artificial-intelligence-ai-application-in-cybersecurity-a-synergistic-approach-to-safeguarding-the-digital-realm

Ugwueze, M. I., Onuoha, J., & Nwagwu, E. J. (2016). Electronic Governance and National Security in Nigeria. Mediterranean Journal of Social Sciences. https://doi.org/10.5901/mjss.2016.v7n6p363

Unaji, E. (2013). Security Agents, Security Threats and the Culture of Impunity: Antithesis to Nigeria's Socio-Economic Development and Political Stability. Journal of Educational and Social Research. https://doi.org/10.5901/jesr.2013.v3n6p147

Zwingina, K., AMB., S. E., Prof., A. E. Z., IGWEBUIKE, P. O., IRABOR, B. I., MARGWA, R., & ONIBIYO, E. R. (2024). Impact of DDoS attacks on critical national information infrastructure and human security in Nigeria. International Journal of Social Science, Management, Peace and Conflict Research, 1(05), 068–084. https://ijsmpcr.com/index.php/ijsmpcr/article/view/65