



Evaluation of A Contextual Cybersecurity Awareness for Polytechnic Students in Nigeria

¹Adamu Zubairu Zubairu, ²Muhammad Ishaq Umar, ¹George Amos, ¹Aliyu Salihu Giza, ²Aisha Ibrahim Galadima

¹Department of Computer Science, Isa Mustapha Agwai I Polytechnic, Lafia, Nasarawa State, Nigeria.

²Department of Computer Science, Federal University of Lafia, Nasarawa State Nigeria.

*Corresponding authors' email: zubairuadam01@gmail.com Phone: +2347066706667

ABSTRACT

Cyber-security threats increasingly affect students who depend on mobile devices, social media, messaging platforms, and online services for academic and personal activities. This study appraised students' perceptions and intended behavior on cyber-security awareness and proposed module for polytechnic students in a Nigerian educational setting. A design-based research-informed approach combined with a descriptive survey evaluation was adopted. Data were collected from 500 students selected through stratified random sampling across five departments at Isa Mustapha Agwai I Polytechnic, Lafia, Nasarawa State, Nigeria. The study assessed students' self-reported cyber-security awareness, cyber-security experiences and practices, perceptions of the contextual learning module, and intended cyber-security behavior. Findings indicated relatively strong awareness of password security and risks associated with unknown files, but comparatively lower awareness of phishing, social engineering, and suspicious-link identification. Students also reported frequent exposure to fake offers, suspicious WhatsApp messages, malicious links, fraudulent OTP/PIN requests, and impersonation. A design-based research-informed approach combined with a descriptive survey design was adopted. The study population comprised 913 students drawn from five selected departments, namely Computer Science (150), Science Laboratory Technology (189), Accounting (216), Library and Information Science (243), and Computer Engineering (115). A sample of 500 students (54.76% of the study population) was selected using stratified random sampling with equal allocation of 100 students from each department. Data were collected using a structured questionnaire based on a five-point Likert scale and analysed using descriptive statistics, including frequency, percentage, mean and standard deviation. The work recommends further implementation of this cyber security awareness module for students' curriculum in Nigeria institutions.

Received: 22 July 2026

Accepted: 05 Sept. 2026

Published: 05 Oct. 2026

Keywords:

Cyber-security Awareness, Contextual Learning, Polytechnic Education, Social Engineering, Isa Mustapha Agwai I Polytechnic

INTRODUCTION

The rapid expansion of digital technologies in higher education has increased students' dependence on online platforms, mobile devices, social media, electronic communication, and digital financial services. While these technologies provide substantial educational and social benefits, they also expose students to cyber-security threats such as phishing, social engineering, malicious links, account compromise, fraudulent online offers, and credential theft. Consequently, cyber-security awareness has become an important component of digital literacy and student education. Previous studies have reported cyber-security awareness gaps among students in educational institutions. Gabra et al. (2020) examined cyber-security awareness among university students and identified weaknesses in students' understanding of important security practices. Similarly, Abdullahi et al. (2021) reported cyber-security awareness concerns among university students in Nigeria, demonstrating the need for stronger cyber-security education within the Nigerian educational environment. More specifically, Okokpujie et al. (2023) investigated Nigerian university students' susceptibility to phishing attacks and reported substantial vulnerability to phishing attempts, highlighting the importance of practical phishing-awareness education. Traditional cyber-security awareness programmes, however, may not adequately reflect the everyday experiences of students within a particular social and technological

environment. Generic training may explain concepts such as phishing, password security, malware, and social engineering without demonstrating how these threats appear in students' actual communication channels and daily activities. The National Institute of Standards and Technology (NIST) recommends structured cyber-security and privacy learning programmes that are relevant to the target audience and support continuous awareness development (Merritt et al., 2024). Recent research on cyber-security education has similarly emphasized the importance of appropriate instructional approaches and learning environments when developing cyber-security knowledge and awareness (Ahmed et al., 2024). The need for contextualization is particularly important in the Nigerian higher-education environment. Students commonly interact through mobile devices and social-messaging platforms, while cyber-security threats may appear in locally recognizable forms, including fake scholarship announcements, fraudulent empowerment or giveaway offers, impersonation of lecturers or student representatives, fake institutional notices, requests for one-time passwords (OTPs), and fraudulent payment notifications. Such examples provide opportunities for cyber-security education to move beyond theoretical explanations towards realistic decision-making scenarios. Scenario-based and interactive approaches can be particularly useful because they allow learners to consider a threat, make a decision, and understand the consequences of that decision.

Emerging research has also identified game-based and experiential approaches as important areas of cyber-security awareness education (Weeratunge et al., 2026). In addition, recent work on African cyber-security education suggests that culturally and contextually appropriate pedagogical approaches can improve the relevance of cyber-security learning for African students (Armah et al., 2026).

Against this background, this study adopts a design-based research (DBR)-informed approach combined with a descriptive survey evaluation. Design-based research provides a useful foundation for developing educational interventions that respond to practical problems within authentic learning contexts (The Design-Based Research Collective, 2003). Rather than treating cyber-security awareness as a purely technical subject, the study focuses on designing a contextual learning module around threats and situations that are familiar to students in a Nigerian polytechnic. The study was conducted at Isa Mustapha Agwai I Polytechnic, Lafia, Nasarawa State, Nigeria, involving 500 students drawn from five departments: Computer Science, Science Laboratory Technology, Accounting, Library and Information Science, and Computer Engineering. The study investigates students' existing self-reported cyber-security awareness and experiences, uses the identified needs to inform the design of a contextual cyber-security awareness module, and evaluates students' perceptions of the module's relevance, usability, and practical applicability.

Research Questions

Accordingly, the study seeks to address the following research questions:

- i. **RQ1:** What cyber-security awareness needs are relevant to students in a Nigerian polytechnic context?
- ii. **RQ2:** How can a contextual cyber security awareness module be designed to address cyber security risks relevant to polytechnic students?
- iii. **RQ3:** How do students perceive the relevance, usability, and practical applicability of the contextual cyber security awareness module?

In view of the above questions (RQ1, RQ2, RQ3), the study examined that, if contextual cyber-security awareness is adopted into student orientation and continuous institutional awareness programmes, the study shall make four main contributions:

- i. It provides an empirical assessment of cyber security awareness needs among students in a Nigerian polytechnic.
- ii. It presents a contextual cyber security awareness module incorporating locally relevant scenarios, including phishing, social engineering, account security, mobile security, online financial fraud, and incident reporting.
- iii. It evaluates students' perceptions of the module across relevance, clarity, usefulness, and practical applicability.

Notably, the study evaluates self-reported awareness, experiences, perceptions, and intended changes in actual cyber-security behavior. The findings therefore view evidence of the perceived relevance see the needs for applicability of contextual cyber-security education while identifying directions for future controlled and longitudinal evaluation.

Cyber-security Awareness Among Students

Cyber-security awareness among students has received increasing attention because students are frequent users of internet-connected devices, online learning platforms, social media, electronic communication, and digital financial services. Although access to digital technologies provides educational benefits, it also exposes students to phishing, social engineering, malware, account compromise, and other cyber threats.

Gabra et al. (2020) investigated cyber-security awareness among university students and identified weaknesses in important cyber-security practices. In the Nigerian context, Abdullahi et al. (2021) examined cyber-security awareness among university students and reported areas requiring improvement in students' cyber-security knowledge and practices. These findings indicate that possession of digital skills does not necessarily imply adequate cyber-security awareness.

Phishing represents a particularly important concern. Okokpujie et al. (2023) investigated Nigerian university students' susceptibility to phishing attacks and found considerable vulnerability to phishing attempts. This suggests that awareness programmes should not focus solely on definitions of cyber threats but should also teach students how to recognise and respond to realistic phishing and social-engineering situations.

Cyber-security Awareness Training and Education

Cyber-security awareness training generally seeks to develop users' ability to recognise threats and adopt safer security practices. NIST's *Building a Cyber-security and Privacy Learning Program* recommends a lifecycle-oriented approach in which awareness, training, education, assessment, and continuous improvement are integrated into an organisational learning programme (Merritt et al., 2024). The guidance also emphasises the importance of evaluating learning programmes and adapting them as cyber-security risks and organisational needs change.

In higher education, cyber-security education may be delivered through formal courses, awareness campaigns, online learning, workshops, simulations, or specialised training programmes. Ahmed et al. (2024) conducted a systematic literature review of how universities teach cyber-security courses online and highlighted the diversity of instructional approaches used in higher education. However, cyber-security education designed primarily around technical concepts may not always address the practical decisions that ordinary students face when using social media, messaging applications, mobile devices, and online services.

Consequently, awareness training should be understandable to students from both computing and non-computing disciplines. A contextual module can present cyber-security concepts using situations that students can readily recognise, thereby reducing the distance between theoretical cyber-security knowledge and everyday digital behavior.

Contextual and Scenario-Based Cyber-security Education

Contextual learning connects educational content with situations that are meaningful to learners. In cyber-security awareness education, this can involve presenting learners with realistic situations and requiring them to identify threats, assess possible consequences, and select appropriate responses.

For example, rather than simply defining phishing, a learning module can present a student with a hypothetical WhatsApp message announcing a scholarship and requesting an OTP or

directing the student to an unfamiliar website. The learner can then be asked to identify warning signs, decide whether to interact with the message, and explain the appropriate response. Similar scenarios can be developed around fake payment alerts, impersonation of lecturers, fraudulent giveaways, malicious mobile applications, and requests for passwords or personal information.

This approach is consistent with the principles of design-based research, which emphasise the relationship between educational theory, designed learning interventions, and authentic educational practice (The Design-Based Research Collective, 2003). Rather than developing an intervention independently of its learning environment, design-based approaches allow educational solutions to be developed around practical problems and subsequently evaluated in context.

Recent research also indicates growing interest in interactive approaches to cyber-security awareness. Weeratunge et al. (2026) conducted a systematic scoping review of game-based cyber-security awareness education and demonstrated the expanding research interest in interactive and engaging approaches to cyber-security learning. Such approaches support the broader argument that cyber-security awareness can benefit from learner-centered activities rather than relying exclusively on conventional information delivery.

African and Nigerian Contexts in Cyber-security Education

Cyber-security education should account for the technological, cultural, institutional, and socioeconomic conditions in which learners operate. A training programme developed for one environment may not automatically address the threats most relevant to students in another environment.

This issue is particularly important in African educational settings. Armah et al. (2026) examined the use of African Indigenous pedagogy and technology for improving African students' understanding of cyber-security and highlighted the value of approaches that are meaningful within African learning contexts. This provides support for moving beyond a one-size-fits-all approach to cyber-security education.

Within the Nigerian student environment, cyber-security threats may occur through communication and service channels that students use routinely. Examples include fraudulent WhatsApp messages, fake scholarship and employment opportunities, social-media impersonation, fake government or institutional announcements, fraudulent payment alerts, and attempts to obtain OTPs, PINs, passwords, or other personal information. These examples are important because cyber-security awareness is more likely to be meaningful when learners can relate security concepts to situations they encounter or recognise.

Cyber-Security Awareness Modules for College and High School Students

This section appraised the importance of public security awareness and this aspect has been studied by researchers a decade ago. Computer Security Institute determined lack of security awareness of people as one of the most critical computer security issues in coming years CSI (2007). In paper by highlights persistent challenges, reported that low customer cybersecurity awareness contributes significantly to phishing and social engineering attacks. Inadequate real-time monitoring systems hinder rapid threat detection and response. The study concludes that while progress has been made, a more integrated and proactive approach is required to further secure Nigeria's financial ecosystem. According to

Kim, E. B. (2013) shows that, counterintuitively, it is the heavy users of digital devices who are usually the least knowledgeable and least aware of cyber security issues and prevention. Attempts to educate people about cyber security risks have surged in the past 5 years (e.g., SANS Institute (2017) & SANS Institute (2017). Also in a work by Franke, U. & Brynielsson, J. (2014) and Vacca, W. A. (2012) reviews of programs developed to improve cyber security awareness and proposed a systemic program for governments and institutions worldwide can create programs to improve cyber awareness ad to reduce cybercrime, such as CyberWatch and US-CERT, to increase awareness and responsiveness to cyber security threats. National Cyber Security Division (NCSD) within the Department of Homeland Security and the National Cyber Security Alliance (NCSA) declared the month of October as Cyber Security Awareness Month in 2004 citing the importance of making the public aware of cyber security issues. Since then many schools, organizations, and businesses adopted it. Also Kim, E. B. (2013) argued that cyber security training is imperative for college students and that survey data can help determine whether problems with security are due to lack of concern or lack of skill (in navigating devices' security settings). Bruijn et al. (2017) discusses that cybersecurity is a public concern receiving insufficient awareness due to its complexity and paradoxes it exhibits in policy making. The authors suggest evidence-based framing for building cyber-security awareness and presents framing strategies for creating societal and political awareness. In another research by Suleiman A. A (2019), the paper examines the categories, types, modes of cybercrime and the sociological implications of these kinds of crimes on or with cyber space which seems to be a serious threat to our entire security. The paper discusses on such activities in relation to universities system in Nigeria and outlined on the laws, measures and recommendations to address the cybercrime and cyber security in the country.

Research Gap

The reviewed literature establishes three important points. First, cyber-security awareness gaps exist among students, including students in Nigerian higher-education institutions (Gabra et al., 2020; Abdullahi et al., 2021; Okokpujie et al., 2023). Second, effective cyber-security education requires structured learning programmes, appropriate instructional approaches, and mechanisms for evaluation (Ahmed et al., 2024; Merritt et al., 2024). Third, interactive, contextual, and culturally relevant approaches provide promising directions for cyber-security awareness education (The Design-Based Research Collective, 2003; Armah et al., 2026; Weeratunge et al., 2026).

However, there remains a practical gap in the development and evaluation of context-specific cyber-security awareness modules for Nigerian polytechnic students. Much of the existing literature focuses on university students, general cyber-security awareness, susceptibility to individual threats such as phishing, or broader cyber-security education approaches. Less attention has been given to integrating multiple student-relevant threats into a single contextual learning module specifically designed for the Nigerian polytechnic environment.

The present study addresses this gap by combining a student needs assessment with the design and evaluation of a contextual cyber-security awareness module. The module integrates phishing, social engineering, password and account security, WhatsApp and social-media security, mobile and malware security, online financial security, safe internet use, and cyber-incident reporting. Its evaluation focuses on

students' perceptions of relevance, usability, clarity, and practical applicability, while intended behavior is treated as self-reported intention rather than demonstrated behavioral change.

Thus, the study extends previous research by moving from simply measuring cyber-security awareness to using identified student needs to inform the design of a contextual educational intervention and evaluating how students perceive that intervention within a Nigerian polytechnic setting.

MATERIALS AND METHODS

Research Design

This study adopted a design-based research (DBR)-informed framework combined with a descriptive survey design. DBR was chosen because it allows educational tools to be developed in close response to authentic, real-world learning problems (The Design-Based Research Collective, 2003). The methodology consisted of two interrelated phases:

- i. **Needs Assessment Phase:** Quantitative baseline measurement of existing student cyber-security knowledge, threat exposure, and digital habits.
- ii. **Intervention & Evaluation Phase:** Qualitative baseline, this examined Administration of the learning module to polytechnic students, followed by structured evaluation of its usability, pedagogical clarity, contextual relevance, and behavioral intent.

Study Location and Target Population

The study was conducted at Isa Mustapha Agwai I Polytechnic, Lafia, Nasarawa State, Nigeria. The target population comprised registered Higher National Diploma (HND) and National Diploma (ND) students enrolled across both computing and non-computing academic faculties during the academic session.

Sample Size and Sampling Technique

The total of 500 students was selected from 913 students, using a stratified random sampling technique to ensure balanced representation across academic disciplines. The sample criteria, used divided population into five key academic departments with total population 913 students; Computer Science, Science Laboratory, Accounting, Library information Science, and Computer Engineering, where computer Science has the total student's population of 150 but 100 were selected at random, Science Laboratory has the total 189 number of student and 100 students were examined for this research, Accounting 216 students, Library information Science 243 and Computer Engineering 115 students, and from each department, we randomly used 100 students for the research as shown below;

- i. Department of Computer Science (n=100)
- ii. Department of Science Laboratory Technology (n=100)
- iii. Department of Accounting (n=100)
- iv. Department of Library and Information Science (n=100)
- v. Department of Computer Engineering (n=100)

Looking into sciences and technical related disciplines, this sampling structure ensured that the module's instructional design was evaluated by students with varying levels of prior technical background. The calculation for the sample collected and percentage is shown below;

Total population = 150 + 189 + 216 + 243 + 115 = 913 students

Sample (n) = 500 students

Sampling percentage = $n/\text{Sum of all students} \times 100$

$(500 \div 913) \times 100 = 54.76\%$

Therefore a sample of 500 students, representing 54.76% of the total population of 913 students, was selected for the study. The description of how the percentage derived is expressed in table 1 below.

Table 1: Departmental Sample Percentages

Department	Number of Students	Population Sample	Sample as % of
Computer Science	150	100	66.67%
Science Laboratory Technology	189	100	52.91%
Accounting	216	100	46.30%
Library & Information Science	243	100	41.15%
Computer Engineering	115	100	86.96%
Total	913	500	54.76%

Design of the Contextual Cyber-security Module

In this section, the contextual cyber-security module appraised, which six core thematic security domains reflecting common digital interaction channels in Nigerian tertiary institutions are observed:

- i. **Phishing & Social Engineering:** Identifying spoofed academic domains, fake scholarship alerts, and fraudulent giveaway portals.
- ii. **Messaging & Social Media Safety:** Securing WhatsApp, Telegram, and Facebook accounts against takeover attacks and SIM-swap fraud.
- iii. **Password & Account Security:** Constructing strong passphrases, avoiding credential reuse, and enabling Multi-Factor Authentication (MFA).

- iv. **Mobile & Malware Security:** Detecting malicious application installers (APKs), rogue Wi-Fi access points, and unauthorized permissions.

- v. **Financial Digital Hygiene:** Recognizing fake POS bank transfer receipts, phishing links disguised as banking portals, and unauthorized One-Time Password (OTP) requests.

- vi. **Incident Reporting:** Standardized procedures for reporting compromised accounts, financial loss, or identity theft to institutional ICT desks and relevant authorities.

Every topic within the module coupled abstract security definitions with a localized "Real-World Scenario Task," forcing students to analyze suspicious text messages,

evaluate link structures, and choose safe operational responses.

Data Collection Instrument and Validation

Data were collected using a structured, self-administered questionnaire divided into four logical sections:

- i. **Section A:** Demographic information and digital device usage habits.
- ii. **Section B:** Baseline self-reported cyber-security awareness and exposure to cyber threats.
- iii. **Section C:** Student evaluation of the contextual module (Relevance, Clarity, Usability, and Practical Applicability).
- iv. **Section D:** Self-reported intended cyber-security behavior and institutional integration support.

The instrument utilized a 5-point Likert scale ranging from 1 (*Strongly Disagree*) to 5 (*Strongly Agree*). Face and content validity were established through expert review by three senior lecturers in Computer Science and Educational Technology. Instrument reliability was established via a pilot test ($n=30$), yielding a Cronbach's alpha (α) coefficient of 0.86, indicating high internal consistency.

Data Analysis

Descriptive statistical analysis—including frequency counts, percentages, means ($\bar{X}$), and standard deviations (SD)—was conducted using SPSS (Version 26.0). A mean threshold of 3.00 was established as the criterion benchmark for positive agreement on all evaluation scales.

RESULTS AND DISCUSSION

This chapter presents the analysis and interpretation of data collected from students of Isa Mustapha Agwai I Polytechnic, Lafia, Nasarawa State. The analysis focuses on respondents' demographic characteristics, cyber-security awareness, cyber-security experiences and practices, perceptions of the proposed contextual cyber-security learning module, and intended cyber-security behaviour.

A total of 500 questionnaires were targeted and analysed, representing 54.76% of the total population of 913 students across the five selected departments. Data were analysed using frequency, percentage, mean and standard deviation. A five-point Likert scale was employed for the attitudinal and perception-based items.

To express the five-point Likert scale, see table 2 below;

Table 2: Questionnaire Response and Interpretation

Scale	Response	Interpretation
5	Strongly Agree	Very High
4	Agree	High
3	Undecided	Moderate
2	Disagree	Low
1	Strongly Disagree	Very Low

Evaluation of the Contextual Cyber-security Module

Following the administration of the contextual cyber-security module, students evaluated the intervention across key pedagogical and technical dimensions. The quantitative

evaluation yielded consistently high ratings across all evaluated parameters, with mean scores ranging from 4.43 to 4.60 on a 5-point Likert scale. See the table 3 below;

Table 3: Student Module Perceptions and Intended Cyber-security Behavior Ratings (N = 500)

Evaluation Dimension	Mean Score ($\bar{X}$)	Standard Deviation (SD)	Interpretation
Contextual Relevance of Scenarios	4.60	0.52	Strongly Agree
Clarity of Module Content	4.52	0.58	Strongly Agree
Practical Applicability to Daily Mobile Use	4.43	0.61	Strongly Agree
Intended Adoption of Digital Hygiene (MFA/Passwords)	4.69	0.48	Strongly Agree
Support for Institutional Orientation Integration	4.30	0.65	Strongly Agree

As shown in Table 1, the contextual relevance of the scenarios received the highest evaluation score ($\bar{X} = 4.60$, $SD = 0.52$), confirming that grounding cyber-security concepts in recognizable, localized situations (e.g., WhatsApp phishing, fake grant portals, POS scams) significantly enhances student engagement and comprehension. The clarity of module content ($\bar{X} = 4.52$, $SD = 0.58$) and practical applicability to daily mobile usage ($\bar{X} = 4.43$, $SD = 0.61$) were similarly rated very high, indicating that non-computing students found the materials accessible and actionable.

Intended Cyber-security Behavior and Institutional Integration

In terms of behavioral intent, students demonstrated strong commitment to implementing security best practices following the learning intervention. Intended adoption of core digital hygiene practices—such as enabling multi-factor

authentication (MFA) and utilizing strong, non-reused passwords—achieved a mean score of 4.69 ($SD = 0.48$).

Subsequently, students expressed overwhelming support for incorporating cyber-security education into formal institutional frameworks ($\bar{X} = 4.30$, $SD = 0.65$). A substantial majority agreed that contextual cyber-security training should be integrated into new student orientation programmes and general studies (GNS) curricula across all polytechnic departments.

Discussion

The findings of this study align closely with prior research highlighting cyber-security awareness deficits among higher education students in Nigeria (Abdullahi et al., 2021; Okokpuije et al., 2023). However, while generic awareness campaigns often struggle to bridge the gap between abstract technical knowledge and practical compliance, the scenario-driven approach evaluated here demonstrated strong learner resonance.

These outcomes support the core tenets of Design-Based Research (The Design-Based Research Collective, 2003), illustrating that educational interventions designed around authentic operational contexts yield higher user acceptability and practical relevance. Furthermore, the strong positive response to localized threat scenarios aligns with findings by Armah et al. (2026), who emphasized the pedagogical value of contextually and culturally aligned cyber-security instruction for African students. The findings also complement recent reviews on interactive and engaging cyber-security learning frameworks (Ahmed et al., 2024; Weeratunge et al., 2026), confirming that active, scenario-based decision-making represents an effective pathway for enhancing digital hygiene in tertiary institutions.

CONCLUSION

This study evaluated a contextual cyber-security awareness tailored to the specific digital habits and threat exposure of polytechnic students in Nigeria. By utilizing design-based research principles, the study moved beyond generic theoretical definitions to present security concepts through locally relevant scenarios involving mobile messaging, social engineering, financial transactions, and academic identity protection.

The evaluation demonstrated that polytechnic students perceive contextual, scenario-based learning as highly relevant, clear, useful, and practical for their daily digital interactions. Furthermore, the intervention fostered strong self-reported intentions to adopt safe digital hygiene practices, such as multi-factor authentication and vigilant link verification. The study concludes that context-specific instructional Module-design offers a viable, engaging, and scalable strategy for addressing cyber-security awareness gaps in Nigerian tertiary education.

RECOMMENDATIONS

Based on the empirical findings, the following recommendations are proposed:

- i. **Institutionalization in Student Orientation:** Polytechnic management at Isa Mustapha Agwai I Polytechnic and similar tertiary institutions should integrate contextual cyber-security awareness modules into mandatory orientation and matriculation programmes for all newly admitted National Diploma (ND) and Higher National Diploma (HND) students.
- ii. **Curriculum Enhancement Across Non-Computing Faculties:** Academic regulatory bodies, such as the National Board for Technical Education (NBTE), should incorporate contextual digital safety and cyber hygiene topics into general studies (GNS) curricula across non-computing disciplines.
- iii. **Establishment of Institutional Incident Reporting Channels:** Polytechnic ICT centers should institute accessible, student-friendly channels (e.g., dedicated WhatsApp helplines or online reporting portals) to enable prompt reporting and mitigation of compromised student accounts or phishing scams.
- iv. **Continuous Micro-Learning Campaigns:** Institutions should deploy continuous micro-learning awareness updates (Academic Module) via

official student communication channels to keep pace with evolving social engineering and mobile fraud techniques.

- v. **Directions for Future Research:** Future studies should implement longitudinal and experimental control-group research designs to quantitatively measure actual (rather than self-reported) behavioral retention and threat-mitigation performance over extended periods.

REFERENCES

- Abdullahi, A. G., Siraj, M. M., Othman, S. H., & Zogaan, W. A. (2021). Cybersecurity awareness of university students in Nigeria: Analysis approach. *Turkish Journal of Computer and Mathematics Education*, 12(12), 3739–3752. <https://doi.org/10.17762/turcomat.v12i12.8152>
- Ahmed, A., Watterson, C., Alhashmi, S., & Gaber, T. (2024). How universities teach cybersecurity courses online: A systematic literature review. *Frontiers in Computer Science*, 6, Article 1499490. <https://doi.org/10.3389/fcomp.2024.1499490>
- Armah, M., Bada, J. K., Ohene-Afoakwa, E., Mensah, F., & Boateng, K. O. (2026). Improving African students' understanding of cybersecurity using African Indigenous pedagogy and technology. *Discover Education*, 5, Article 587. <https://doi.org/10.1007/s44217-026-01465-2>
- Gabra, A. A., Sirat, M. B., Hajar, S., & Dauda, I. B. (2020). Cyber security awareness among university students: A case study. *International Journal of Advanced Science and Technology*, 29(10s), 767–776.
- Merritt, M., Hansche, S., Ellis, B., Nethery Snyder, J., Sanchez-Cherry, K., & Walden, D. (2024). *Building a cybersecurity and privacy learning program* (NIST Special Publication 800-50 Rev. 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-50r1>
- Okokpuije, K., Kennedy, C. G., Nnodu, K., & Noma-Osaghae, E. (2023). Cybersecurity awareness: Investigating students' susceptibility to phishing attacks for sustainable safe email usage in academic environment (A case study of a Nigerian leading university). *International Journal of Sustainable Development and Planning*, 18(1), 255–263. <https://doi.org/10.18280/ijstdp.180127>
- The Design-Based Research Collective. (2003). Design-based research: An emerging paradigm for educational inquiry. *Educational Researcher*, 32(1), 5–8. <https://doi.org/10.3102/0013189X032001005>
- Weeratunge, N. H., Hjelsvold, R., & Katt, B. (2026). A systematic scoping review on game-based cybersecurity awareness education. *International Journal of Information Security*, 25, Article 71. <https://doi.org/10.1007/s10207-026-01239-9>
- Okikiola, F. M., Arogundade, T. S., Onadokun, I., Oladiboye, O. E., & Adetunji, S. K. (2026). Strengthening financial integrity: The role of cybersecurity in mitigating financial fraud in Nigeria's banking sector. *FUDMA Journal of Sciences*, 10(2), 175-183.

CSI (2007). "Computer crime and security survey 2007". Computer Security Institute, retrieved April 1, 2016 from <http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf>

Kim, E. B. (2013), "Information Security Awareness Status of Business College: Undergraduate Students". *Information Security Journal: A Global Perspective*, 22(4), 171-179.

Ahmad, A. S. (2019). CYBER CRIME AND THE SOCIOLOGICAL IMPLICATION IN THE NIGERIA'S TERTIARY EDUCATION SYSTEM. *FUDMA JOURNAL OF SCIENCES*, 3(1), 249-257.

SANS Institute (2017), Security Awareness Report. Retrieved 12/8/ 2017 from <https://securingthehuman.sans.org/media/resources/STHSecurityAwarenessReport-2017.pdf>

Verizon (2015), Data Breach Investigation Report. Verizon, retrieved April 14, 2016 from

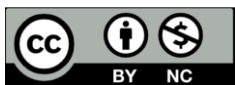
http://www.verizonenterprise.com/DBIR/2015/?utm_source=pr&utm_medium=pr&utm_campaign=dbir2015

Vacca, W. A. (2012), " Military Culture and Cyber Security. Survival" (00396338), 53(6), 159-176. doi: <https://doi.org/10.1080/00396338.2011.636520>

Franke, U. & Brynielsson, J. (2014). "Cyber situational awareness – A systematic review of the literature". *Computers & Security*, 46, 18- 31.

De Bruijn, H. & Janssen, M. (2017). "Building Cybersecurity Awareness: The need for evidence-based framing strategies". *Government Information Quarterly*, 34 (1), 1-7.

Peker, Y., Ray, L., & Da Silva, S. (2018, June). Online cybersecurity awareness modules for college and high school students. In *2018 National Cyber Summit (NCS)* (pp. 24-33). IEEE.



©2026 This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International license viewed via <https://creativecommons.org/licenses/by/4.0/> which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is cited appropriately.