Assessment of Pre-Service Business Education Students' Awareness And Attitude Toward Cybersecurity Education In Colleges Of Education In Southwest Nigeria

(Penilaian Kesedaran Dan Sikap Pelajar Pendidikan Perniagaan Pra-Perkhidmatan Terhadap Pendidikan Keselamatan Siber Di Kolej Pendidikan Di Barat Barat Nigeria)

BILQEES MOPELOLA OLADUNNI-MOHAMMAD* &
OLAJUMOKE DAMILOLA ONIFADE

Abstract

The rapid digitalisation of Nigerian education and business has heightened the urgency of cybersecurity literacy, particularly among pre-service teachers who will shape the digital habits of future generations. This study assessed the awareness and attitude of pre-service business education students toward cybersecurity education in selected Federal Colleges of Education in Southwest Nigeria. A descriptive survey design was adopted, with 149 respondents drawn through purposive sampling from the Federal College of Education (Technical), Akoka; Federal College of Education, Osiele; and Federal College of Education (Special), Oyo. Data were collected using the researcher-developed Cybersecurity Awareness and Attitude Questionnaire (CAATQ), structured on a four-point Likert scale, and analysed through frequency counts, percentages, means and standard deviations, while research hypotheses were tested using multiple regression analysis at a 0.05 level of significance. Findings revealed that the majority of respondents (87.2%) were aware of cybersecurity education, with female students constituting 61.7% of the sample and a strong concentration in Marketing and Accounting Education. Attitudinal analysis indicated moderate anxiety (mean = 2.56), cautious confidence (mean = 2.61) and notable positive interest (mean = 2.64) in acquiring further cybersecurity knowledge, though scores on collaborative learning were comparatively lower. The study concludes that, while awareness and disposition are encouraging, structured, tiered and discipline-specific cybersecurity training is needed to convert this readiness into competence. Practical, gender-sensitive and hands-on cybersecurity modules should therefore be embedded into the business education curriculum.

Keywords: Cybersecurity education; pre-service teachers; business education; awareness; attitude; Southwest Nigeria

Abstrak

Digitalisasi pesat dalam sektor pendidikan dan perniagaan di Nigeria telah meningkatkan keperluan mendesak terhadap literasi keselamatan siber, khususnya dalam kalangan guru praperkhidmatan yang bakal membentuk amalan digital generasi akan datang. Kajian ini menilai tahap kesedaran dan sikap pelajar praperkhidmatan dalam bidang pendidikan perniagaan terhadap pendidikan keselamatan siber di beberapa Kolej Pendidikan Persekutuan terpilih di Barat Daya Nigeria. Reka bentuk tinjauan deskriptif telah digunakan, melibatkan 149 orang responden yang dipilih melalui pensampelan bertujuan daripada Federal College of Education (Technical), Akoka; Federal College of Education, Osiele; dan Federal College of Education (Special), Oyo. Data dikumpulkan menggunakan soal selidik yang dibangunkan oleh penyelidik, iaitu *Cybersecurity*

Awareness and Attitude Questionnaire (CAATQ), yang distrukturkan berdasarkan skala Likert empat mata. Data dianalisis menggunakan kekerapan, peratusan, min dan sisihan piawai, manakala hipotesis kajian diuji melalui analisis regresi berganda pada aras signifikan 0.05. Dapatan kajian menunjukkan bahawa majoriti responden (87.2%) mempunyai kesedaran terhadap pendidikan keselamatan siber. Pelajar perempuan membentuk 61.7% daripada keseluruhan sampel, dengan tumpuan yang ketara dalam bidang Pendidikan Pemasaran dan Pendidikan Perakaunan. Analisis sikap menunjukkan tahap kebimbangan yang sederhana (min = 2.56), keyakinan berhati-hati (min = 2.61) dan minat positif yang ketara (min = 2.64) untuk memperoleh pengetahuan lanjut berkaitan keselamatan siber. Walau bagaimanapun, skor bagi pembelajaran kolaboratif didapati secara relatifnya lebih rendah. Kajian ini merumuskan bahawa, meskipun tahap kesedaran dan kecenderungan pelajar adalah memberangsangkan, latihan keselamatan siber yang berstruktur, berperingkat dan khusus mengikut disiplin masih diperlukan bagi menukar kesediaan tersebut kepada kompetensi sebenar. Oleh itu, modul keselamatan siber yang bersifat praktikal, peka gender dan berasaskan latihan amali wajar diintegrasikan ke dalam kurikulum pendidikan perniagaan.

Kata kunci: pendidikan keselamatan siber; guru praperkhidmatan; pendidikan perniagaan; kesedaran; sikap; Barat Daya Nigeria.

Introduction

In the 21st century, cybersecurity has emerged as a fundamental pillar for the digital transformation of education and business (Ayanwale, Sanusi, Molefi, & Otunla, 2024). As societies become increasingly dependent on digital systems, individuals are more exposed to various cyber threats such as phishing, identity theft, ransomware, data breaches, and cyberbullying. This reality has elevated cybersecurity education from a technical concern to a societal priority, particularly in educational institutions where young digital natives are being prepared for the demands of a technology-driven world (Apata, Adeniyi, Ajiwoju, & Adeosun, 2025; Ameen, Liu, & Ahmad, 2021). The World Economic Forum (2022) reported that cybersecurity threats are evolving at an unprecedented rate, with human error accounting for more than 90% of breaches highlighting the crucial role of education in promoting digital safety. Educators, particularly those in training, must therefore be well-equipped not just with basic ICT skills, but also with sound knowledge of digital ethics, cyber hygiene, and online risk management (Chigada & Madzinga, 2021). As future professionals, pre-service business education teachers are expected to serve not only as knowledge transmitters but also as role models for safe digital practices in both classrooms and workplaces.

In Nigeria, the growing integration of digital technologies into teaching and learning has amplified the need for cybersecurity literacy. Government initiatives, such as the National Digital Economy Policy and Strategy (2020–2030), have prioritized digital skills development across education sectors. However, there is a widening gap between policy and implementation, particularly in teacher preparation programs (Tew, 2019). While many colleges of education have incorporated ICT modules into their curriculum, cybersecurity-specific training remains limited or entirely absent (Ayanwale et al., 2024). This is concerning, given the increasing reliance on internet-based tools for research, instruction, assessment, and communication. Furthermore, pre-service business education teachers in Nigeria operate at the intersection of education and enterprise are two domains that are especially vulnerable to cybercrime. Their dual roles demand both pedagogical

and practical proficiency in cybersecurity principles such as data privacy, secure online transactions, and responsible use of social media. Yet, few empirical studies have assessed how well-prepared these future educators are in navigating such risks (Olusola & Ayo, 2021). A lack of cybersecurity awareness or a poor attitude toward digital safety could undermine not only their own professional integrity but also the security of their students and future employers.

Globally, studies have shown that attitudes towards cybersecurity significantly affect behavioral intentions and the adoption of safe practices (Ameen et al., 2021). Negative emotions like fear, anxiety, or skepticism can lead to resistance, while confidence and positive experiences can enhance engagement. This duality makes it essential to evaluate both the knowledge and the attitudinal disposition of pre-service teachers toward cybersecurity education. This study therefore investigates the level of cybersecurity knowledge and the attitudes towards cybersecurity education among pre-service business education teachers in federal colleges of education in Southwest Nigeria.

Statement of the Problem

Cybersecurity threats are escalating globally, affecting not only businesses and governments but also educational institutions. As the use of digital tools becomes ubiquitous in Nigerian classrooms, the need for cybersecurity education becomes increasingly critical. Business education, with its integration of ICT, places pre-service teachers at the forefront of digital engagement. However, questions remain regarding their preparedness to navigate, understand, and teach cybersecurity threats. Preliminary observations suggest that while pre-service teachers interact daily with digital tools, their level of cybersecurity knowledge and the attitudes they hold toward cybersecurity education remain uncertain (Pusey & Sadera, 2011; Digital Security in Educational Contexts, 2024). Research has consistently shown that pre-service teachers tend to have poorly developed digital skills in relation to cybersecurity despite regular engagement with technology (Computers in the Schools, 2024), and findings from Nigerian institutions similarly revealed that students possessed only a rudimentary understanding of cybersecurity and were largely unaware of how to protect their data (Ahamed et al., 2024). Without adequate knowledge and a positive attitude toward cybersecurity, these future educators may struggle to protect themselves, their students, and their institutions from digital risks, as both in-service and pre-service teachers are considered vulnerable to cybersecurity attacks and mostly ill-prepared to prevent them (Dawson et al., 2022; Ferrari & Punie, 2013).

Furthermore, current teacher education programs appear to lack sufficient emphasis on cybersecurity training, as efforts within pre-service teacher education remain almost non-existent despite scholars identifying this knowledge gap over a decade ago (Pusey & Sadera, 2011; Dawson et al., 2022). Research findings consistently reveal low levels of digital security competence among future teachers and training deficiencies in preparing them to address this critical area (IJIET, 2026; Digital Security in Educational Contexts, 2024). This is particularly concerning in Nigeria, where the rapid integration of digital technologies in higher education has significantly increased exposure to cyber threats, and where cybersecurity awareness among students and educators remains insufficient for ensuring safe digital practices (Springer Nature, 2025; IIARD Journals, 2025). This study, therefore, seeks to assess the awareness and attitude towards

cybersecurity among pre-service business education teachers in selected federal colleges of education in Southwest Nigeria.

Purpose of the study

Specifically, the study will examine

1. pre-service business education teachers in colleges aware of cybersecurity education
2. pre-service business education students' attitude towards cybersecurity education in colleges of Education.

Research Questions

The following research questions will be answered

1. Are pre-service business education teachers in colleges aware of cybersecurity education
2. What is the attitude of pre-service business education students towards cybersecurity education in colleges of Education

Methodology

This study adopted a descriptive survey research design, which is appropriate for collecting data on current conditions, practices, and opinions without manipulating variables. The descriptive survey method was selected because it allows for the collection of extensive information regarding the awareness and attitudes towards cybersecurity education among pre-service Business Education teachers in Southwest Nigeria. The research was conducted in the Southwest geopolitical zone of Nigeria, which includes the States of Oyo, Ogun, Ekiti, Ondo, Osun, and Lagos. This region is known for hosting several Colleges of Education and producing a significant number of qualified teachers. Three federal Colleges of Education were purposively selected: Federal College of Education (Technical), Akoka, Lagos State, Federal College of Education, Osiele, Ogun State and Federal College of Education (Special), Oyo, Oyo State. The target population comprised 212 pre-service Business Education teachers enrolled in the selected federal Colleges of Education within the 2024/2025 academic session. These participants were drawn from the School of Technical and Vocational Education, specifically those registered in Business Education programs. A purposive sampling technique was employed to select the three federal Colleges of Education based on their relevance and program offerings. All 212 pre-service Business Education students from these colleges formed the sample for the study, thereby ensuring full population participation. The sampling was guided by institutional records available for the 2023/2024 academic session.

Table 1: Distribution of Stakeholders in College of Education

S/N	Colleges of Education	Students	Sampled	Facilitators

1	Federal College of Education (Special), Oyo	83	52
2	Federal College of Education, Osiele, Abeokuta	72	37
3	Federal College of Education (Technical) Akoka	57	62
Total		**212**	**149**

The distribution of stakeholders in the selected Federal Colleges of Education in Southwest Nigeria reveals a strategic sampling of participants for this study. A total of 212 pre-service Business Education students were enrolled across the three selected colleges, and a sample of 149 respondents was drawn from this population. At the Federal College of Education (Special), Oyo, there were 83 registered Business Education students during the 2023/2024 academic session. Out of this number, 52 students were sampled to participate in the study. This institution contributed substantially to the overall sample, accounting for approximately one-third of the respondents. Its selection reflects its long-standing reputation for teaching, particularly in special education and vocational studies. The Federal College of Education, Osiele, Abeokuta, had a total of 72 Business Education students, from which 37 were sampled. Although the student population here was slightly lower than in Oyo, its inclusion in the study was essential to ensure a balanced representation across the region. The sampled number reflects roughly a quarter of the total study participants. In contrast, the Federal College of Education (Technical), Akoka, while having the smallest total student population among the three (57 students), contributed the largest sample size of 62. This anomaly suggests that the sample might have included not only students but possibly facilitators or additional participants relevant to the study objectives. The high participation rate from Akoka highlights the college's strong engagement with technology-based education, aligning well with the study's focus on cybersecurity education. The total sample of 149 participants was drawn purposively from a population of 212 pre-service Business Education teachers across three federal Colleges of Education in Southwest Nigeria. The sampling ensured a broad and representative distribution, enhancing the validity of the findings and providing a solid foundation for examining knowledge and attitudes toward cybersecurity education among future educators in the region.

This study utilizes two well-structured research instruments to effectively evaluate the knowledge and awareness of cybersecurity among pre-service Business Education students. The principal instrument, titled the *Cybersecurity awareness and attitude towards Questionnaire (CAATQ)*, is divided into sections beginning with demographic information, followed by comprehensive items assessing participants' levels of cybersecurity awareness and attitude. The questionnaire employs a 4-point Likert scale ranging from *Strongly Agree (4)* to *Strongly Disagree (1)*. To facilitate the data collection process, the researcher obtained an introductory letter from her department. With this hand, she visited each of the selected Federal Colleges of Education to request official permission to involve their students in their study. Prior to administering the instrument, informed consent was obtained from all targeted participants to ensure voluntary participation. Additionally, a brief explanation outlining the purpose of the study was included on the front page of the questionnaire to further inform the respondents. Once permission was granted, participants were selected based on the sampling procedure detailed earlier under "Sample and Sampling Techniques." The researcher explained the objectives and goals of the study to the selected pre-

service teachers before distributing the questionnaire. To support the data collection process, two research assistants were recruited from each participating college. These assistants were briefed on the study's purpose and received a one-day training session on the proper procedure for administering the instrument and interacting with participants. Following this, the questionnaires were distributed and collected by the researcher, with assistance from the trained research personnel. The data collected in this study were analyzed using quantitative techniques. Descriptive statistics, including frequency counts, percentages, means, and standard deviations, were employed to summarize and interpret responses related to the research questions. To test the research hypotheses, inferential statistics specifically, multiple regression analysis were applied at a 0.05 level of significance. This approach enabled the researcher to identify patterns and relationships within the data, providing a comprehensive understanding of the variables under investigation.

Result

Table 2: Respondents from Federal Colleges of Education

S/N	Colleges of Education	Sampled	%
1	Federal College of Education (Special), Oyo	52	34.44
2	Federal College of Education, Osiele, Abeokuta	37	24.50
3	Federal College of Education (Technical) Akoka	62	41.06
Total		**149**	**100**

Table 2 presents the distribution of respondents drawn from three Federal Colleges of Education in Southwest Nigeria. The Federal College of Education (Special), Oyo, accounted for 52 participants, representing 34.44% of the total sample. This makes a considerable contribution to the overall dataset. The Federal College of Education, Osiele, Abeokuta, contributed 37 participants, which constitutes 24.50% of the total respondents indicating a moderate level of representation. Meanwhile, the Federal College of Education (Technical), Akoka, recorded the highest participation with 62 respondents, making up 41.06% of the sample. Altogether, the three institutions yielded a total of 149 respondents. The distribution underscores a balanced and inclusive approach to data collection, with each college contributing proportionally to ensure diverse perspectives within the study population.

Table 3: Respondents based on Course of Study

S/N	**Course of Study**	**F**	**%**
1	Accounting Edu	65	43.6
2	OTME	7	4.7
3	Marketing	67	45.0
4	Entrepreneurial	10	6.7
	Total	149	100

Table 3 highlights the distribution of respondents according to their respective courses of study. Out of the total 149 participants, Marketing recorded the highest number of students, with 67 respondents, accounting for 45.0% of the sample. This was closely followed by Accounting Education, which had 65 students, representing 43.6%. These two courses clearly dominate the academic landscape among the respondents. In contrast, Entrepreneurial Studies had 10 students (6.7%), while Office Technology and Management Education (OTME) had the fewest participants, with 7 students (4.7%). Collectively, students in Marketing and Accounting Education constituted 88.6% of the total sample, indicating a significant concentration in these areas of specialization.

Table 4: Respondents based on Gender

S/N	Gender	F	%
1	**Male**	**57**	**38.3**
2	**Female**	**92**	**61.7**
	Total	**149**	**100**

Table 4 presents the gender distribution of the 149 respondents in the study. Female participants constituted the majority, numbering 92 and representing 61.7% of the total sample. Male respondents accounted for 57 participants, making up 38.3% of the total. This reveals a significant gender imbalance in favor of female students, with a ratio of nearly three females to every two males.

Research Question 1: Are pre-service business education teachers in colleges aware of cybersecurity education

S/N	Statement	Aware F (%)	Not Aware F (%)
1.	I am aware of cybersecurity education	130 (87.2)	19 (12.8)

The findings reveal that a substantial proportion of pre-service business education teachers are aware of cybersecurity education. Out of the total respondents, 130 (87.2%) acknowledged their awareness, while only 19 (12.8%) reported being unaware. This indicates that most participants have some familiarity with cybersecurity education. However, the small but notable percentage of respondents lacking awareness highlights the need for further efforts to ensure comprehensive understanding across all pre-service teachers.

Research Question 3: What is the attitude (Anxiety, confidence and likeness) of pre-service business education teachers in colleges of education towards cybersecurity education

S/N	Statement (Anxiety)	Means	SD
1.	Cybersecurity education does not scare me at all	2.63	1.50
2	Cybersecurity would make me nervous online	2.48	1.46
3	I do not feel threatened when others talk about cybersecurity	2.57	1.26
4	I do not feel aggressive and hostile towards cybersecurity	2.63	1.41
5	It wouldn't bother me at all to take Cybersecurity courses	2.50	1.44

6	Cybersecurity makes me feel uncomfortable	2.38	1.48
7	I would feel at ease in a Cybersecurity class	2.84	1.55
8	I feel uncomfortable working online without considering cyber threats	2.60	1.47
9	Cybersecurity makes me feel uneasy and confused	2.41	
Confidence			
10	I am not good at tackling Cybersecurity issues	2.50	0.37
11	Generally, I would feel okay about trying a new technology without threat	2.88	0.33
12	I can do advanced work amidst Cybersecurity	2.53	1.50
13	I am sure I could learn Cybersecurity language	2.83	1.46
14	I could get good grades in Cybersecurity courses	2.63	1.25
15	I do not think I could handle Cybersecurity course	2.24	1.41
16	I have a lot of confidence when it comes to working with online	2.63	1.44
	Likeness		
17	I would like to have more knowledge about Cybersecurity	2.81	0.33
18	The challenge of solving problems with Cybersecurity does not appeal to me	2.53	1.50
19	I think understanding Cybersecurity would be enjoyable	2.67	1.46
20	Cybersecurity problems do not appeal to me	2.67	1.25
21	When there's a problem on Cybersecurity that I can't immediately solve, I will stick with it until I have the answer	2.57	1.41
22	Once I start to work with Cybersecurity, I will find it hard to stop	2.63	1.44
23	If a problem is left unsolved in a Cybersecurity case, I would find it hard to continue to think about it afterward	2.59	1.48
24	I do not enjoy talking with others about Cybersecurity	2.34	1.55
25	I do not enjoy talking with others about Cybersecurity	2.92	1.47

Anxiety: The average mean is approximately **2.56**.
Confidence: The average mean is approximately **2.61**.
Likeness: The average mean is approximately **2.64**.

The study examined the attitudes of pre-service business education teachers towards cybersecurity education through three key dimensions: anxiety, confidence, and likeness. The findings reveal a generally neutral to moderately positive disposition towards cybersecurity education among respondents.

Regarding anxiety levels, the average mean score of 2.56 suggests a moderate level of apprehension. While some participants expressed comfort with cybersecurity concepts - as evidenced by higher agreement scores for statements like "I would feel at ease in a Cybersecurity class" (2.84) and "Cybersecurity education does not scare me at all" (2.63) others reported feelings of discomfort. This is reflected in lower scores for items such as "Cybersecurity makes me feel uncomfortable" (2.38) and "Cybersecurity makes me feel uneasy and confused" (2.41). The relatively high standard deviations (ranging from 1.26 to 1.55) across these anxiety-related items

indicate significant variation in individual responses, suggesting that while some teachers approach cybersecurity with confidence, others experience notable apprehension.

The confidence dimension yielded an average mean score of 2.61, indicating moderate self-assurance among respondents. Participants showed strong confidence in their ability to learn cybersecurity concepts ("I am sure I could learn Cybersecurity language" 2.83) and in working with new technologies ("Generally, I would feel okay about trying a new technology without threat" 2.88). However, some respondents expressed doubts about their capabilities, particularly in handling advanced cybersecurity coursework ("I do not think I could handle Cybersecurity course" - 2.24). The generally moderate confidence levels, coupled with the variation in responses, suggest that while many pre-service teachers believe in their potential to develop cybersecurity skills, others may require additional support and encouragement.

In terms of likeness or interest in cybersecurity, the average mean score of 2.64 reflects a modest but positive inclination. The highest level of interest was expressed in acquiring more cybersecurity knowledge (2.81), while the enjoyment of discussing cybersecurity topics with others received the lowest scores (2.34 and 2.92, though this latter score appears anomalously high and may warrant verification). The moderate scores for persistence in solving cybersecurity problems (2.57) and enjoyment of cybersecurity challenges (2.67) suggest that while many respondents see value in cybersecurity education, their enthusiasm may be tempered by perceived difficulties or lack of immediate relevance to their teaching roles.

The findings collectively suggest that pre-service business education teachers generally recognize the importance of cybersecurity education but approach it with varying degrees of comfort and confidence. The moderate scores across all three dimensions indicate neither strong enthusiasm nor significant resistance, but rather a cautious openness to cybersecurity education. This attitude profile suggests that well-designed, supportive training programs could effectively enhance both competence and confidence in cybersecurity matters among these future educators. The variation in responses highlights the need for differentiated instructional approaches that can address the diverse comfort levels and learning needs within this population.

Discussion of Findings

Awareness of Cybersecurity

The finding that 87.2% of the pre-service business education teachers in the three Federal Colleges of Education are aware of cybersecurity is encouraging and broadly aligns with the trajectory observed in recent literature, although it sits at the more optimistic end of reported results. Zwilling, Klien, Lesjak, Wiechetek, Cetin and Basim (2022) similarly found that internet users across Israel, Slovenia, Poland and Turkey possess adequate cyber threat awareness, suggesting that exposure to digital tools and media campaigns may be cultivating baseline awareness independently of formal instruction. In the African context, Chandarman and Van Niekerk (2017) reported comparable awareness levels among tertiary students in South Africa, while Garba, Siraj, Othman and Musa (2020) and Garba, Siraj and Othman (2022) found only moderate awareness

among Nigerian university students in the North-East, with females being more vulnerable to cyber-attacks. The higher awareness recorded in the present study may therefore reflect the regional advantage of Southwest Nigeria in terms of digital infrastructure, internet penetration, and exposure to cybersecurity discourse, rather than the success of any deliberate curricular intervention. Nevertheless, the 12.8% unaware minority remains consequential: as Pusey and Sadera (2011), in the seminal work that continues to anchor this field, cautioned, pre-service teachers who themselves lack cybersecurity understanding cannot be expected to model or teach digital safety to their future learners.

Anxiety toward Cybersecurity Education

The moderate anxiety mean of 2.56 indicates that while respondents are not paralysed by fear of the subject, a significant portion experiences apprehension, particularly toward its more technical dimensions. This pattern echoes Pusey and Sadera's (2012) focus-group findings, where pre-service teachers expressed concerns about their preparedness to teach cyberethics, cybersafety, and cyber-security (C3) and worried about the reactions of administrators and parents to emotionally charged content. More recently, a Springer-published study during the COVID-19 pandemic likewise reported that pre-service teachers were limited in their awareness of cyber security threats and risks likely to affect their use of digital technologies, a limitation that translates directly into anxiety when they are asked to teach the subject. The implication of the present finding is that anxiety in this cohort is not a generalised aversion but a competency-related discomfort that is amenable to remediation through structured, scaffolded instruction.

Confidence in Cybersecurity Learning

The confidence mean of 2.61, reflecting cautious optimism about learning basic concepts but reduced assurance for advanced applications, mirrors a pattern that has become almost universal in literature. A K-12 educator survey reported by The Learning Counsel (2023) found that 86 percent of teachers had received less than six hours of cybersecurity training and only 23 percent felt confident teaching cybersecurity concepts a stark reminder that confidence gaps persist even in better-resourced contexts. The K-12 GenCyber teacher study published in 2022 demonstrated that perceived self-confidence in designing and implementing cybersecurity lessons rose significantly after a structured workshop, suggesting that the confidence gap observed among Nigerian pre-service teachers is not a fixed trait but a function of training exposure. Zwilling et al. (2022) further argue that cybersecurity knowledge is the strongest predictor of cyber-protective behaviour, independent of country or gender, reinforcing the imperative to convert this moderate confidence into competence through hands-on practice.

Likeness toward Cybersecurity

The likeness mean of 2.64 the highest of the three attitudinal dimensions, provides the most encouraging signal in the study. Respondents are willing and even eager to learn more, which aligns with the Lesotho structural-equation study published in 2023, which examined pre-service teachers' intention to learn about cybersecurity in the Global South and found similarly positive dispositions despite institutional constraints. Muniandy, Muniandy and Samsudin (2017), in their Malaysian study, also reported that higher-education students display a generally positive

orientation toward cybersecurity learning when its personal relevance is made explicit. However, the comparatively lower scores on the collaborative-learning items in the present study deserve attention. The 2024 systematic review on cybersecurity awareness in schools highlights that strategies such as the integration of digital tools, embedding cybersecurity within K-12 curricula, and targeted training for educators significantly enhance engagement, but the same review notes that group-based and socially intensive formats sometimes fail to land with learners who feel exposed by their lack of technical fluency. This may explain why Nigerian pre-service teachers prefer individualised, practical engagement to overtly collaborative formats a preference instructional designer in teacher education programmes must respect.

Conclusion

This study reveals that pre-service business education teachers across three Federal Colleges of Education in Southwest Nigeria demonstrate high cybersecurity awareness and moderately positive attitudes (likeness, indicating cautious optimism and genuine interest in acquiring further knowledge). However, the minority who remain unaware, coupled with reduced confidence in advanced applications and weaker scores on collaborative learning, expose critical gaps that teacher education programs must address through tiered curricula, hands-on practical experiences, and discipline-specific adaptations sensitive to gender and specialisation differences. While the regional scope of the study warrants broader, longitudinal, and comparative research, the findings affirm that Nigerian teacher education has a receptive foundation on which to build and strategically leveraging this readiness will equip future business educators with the competencies needed to foster a digitally literate and secure society through their classrooms.

Recommendations

Based on the study's findings, the following recommendations are proposed to enhance cybersecurity education for pre-service business education teachers in Nigerian colleges of education:

1. Cybersecurity education should be systematically integrated into the teacher training curriculum by Ministries of Education
2. Colleges of education should organize workshops and certifications for teacher educators on cybersecurity fundamentals and pedagogy.
3. institutional should Mandate cybersecurity modules in national teacher education standards for business programs.

References

Ameen, N., Liu, H., & Ahmad, N. (2021). Closing the digital divide in the post-COVID-19 era: A review of the digital literacy landscape and policy directions. *Government Information Quarterly, 38*(4), 101620. https://doi.org/10.1016/j.giq.2021.101620

Apata, S. B., Adeniyi, J. T., Ajiwoju, J. A., & Adeosun, K. K. (2025). Digital transformation in teaching: The preparedness of in-service teachers in Nigeria for the Fourth Industrial

Revolution (4IR). *British Journal of Contemporary Education, 5*(1). Retrieved from https://abjournals.org/bjce

Ayanwale, M. A., Sanusi, I. T., Molefi, R. R., & Otunla, A. O. (2024). A structural equation approach and modelling of pre-service teachers' perspectives of cybersecurity education. *Education and Information Technologies, 29*, 3699–3727. https://doi.org/10.1007/s10639-023-11973-5

Chigada, J., & Madzinga, R. (2021). Digital literacy and cybersecurity awareness among students in South African universities. *South African Journal of Information Management, 23*(1), a1292. https://doi.org/10.4102/sajim.v23i1.1292

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340. https://doi.org/10.2307/249008

Olusola, A. A., & Ayo, C. K. (2021). Cybersecurity awareness and behaviour of university students: The Nigerian experience. *Information and Computer Security, 29*(3), 402–421. https://doi.org/10.1108/ICS-02-2020-0028

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Tew, P. A. D. (2019). Cybersecurity education in Nigeria: A pre-requisite for the life-long learner in the 21st century. *The COLLOQUIUM, 7*(1), 38–45. Retrieved from https://www.ajol.info/index.php/colloq/article/view/238718

World Economic Forum. (2022). *Global cybersecurity outlook 2022*. Retrieved from https://www.weforum.org/reports/global-cybersecurity-outlook-2022

Bilqees Mopelola Oladunni-Mohammad*
Department of Technology and Vocational Education
Faculty of Education
University of Lagos
E-mail: mopelolamohammad15@gmail.com

Olajumoke Damilola Onifade
Department of Technology and Vocational Education
Faculty of Education
University of Lagos

*Corresponding Author: Bilqees Mopelola Oladunni-Mohammad

Received: 09 November 2025
Reviewed: 10 February 2026
Accepted: 30 April 2026
Published: 30 May 2026