Journal of Educational Sciences
Journal homepage: https://jes.ejournal.unri.ac.id/index.php/JES

P-ISSN 2581-1657
E-ISSN 2581-2203

Enhancing Students' Awareness and Interest in Information Security: The Role of Culturally Relevant Instructional Strategy

[1]Olasunkanmi A. Gbeleyi, [2]Jessie Yao Foli, [3]Stephen. O. Akintolure, [4]Adekunle I. Oladejo & [5]Olanrewaju Olasupo Ariyibi

[1,4]Africa Centre of Excellence for Innovative and Transformative STEM Education, Lagos State University, Ojo, 102101, Nigeria
[2]University of Professional Studies, Accra, Ghana
[3]Department of Educational Technology, College of Information and Technology Education, Lagos State University of Education, Oto/Ijanikin.
[5]Department of Science and Technology Education, Lagos State University, Ojo, 102101, Nigeria

ARTICLE INFO

Article history:

Received: 28 Aug 2024
Revised: 03 Jan 2025
Accepted: 04 Jan 2025
Published online: 24 Jan 2025

Keywords:

Awareness
Cultural Innovation
Culturo-Techno-Contextual Approach (CTCA),
Information Security, Interest

* *Corresponding author:*

E-mail: gbeleyiadio.edu@gmail.com

Article Doi:

Doi: https://doi.org/10.31258/jes.9.1.p.288-304

A B S T R A C T

This study examines the integration of information security awareness and interest in educational settings, focusing on how classroom practices can align with cultural relevance and innovative teaching methods. It compares two teaching approaches to assess their impact on awareness and student interest in ICT, particularly Information Security. It specifically evaluates the Culturo-Techno-Contextual Approach (CTCA), which combines culture, technology, and context, to enhance Ghanian Junior High School students' awareness and interest in Information Security. The study investigates whether CTCA can foster deeper learning and boost students' engagement in information security. A total of 106 students participated, with 54 in the experimental group and 52 in the control group. As random assignment was not feasible, an ancova analysis was conducted, using pretest scores as a covariate. The findings showed that the CTCA method was more effective than traditional teaching, with a significant improvement in students awareness and interest in Information Security ($F(1, 103) = 3.91$; $p = .05$). The intercept was highly significant ($p < 0.001$). Based on these results, the study suggests adopting the CTCA approach in Sub-Saharan Africa to improve students' awareness and interest in ICT and related subjects.

1. Introduction

Information Security (IS) awareness is a critical component in addressing human risks, perceptions, and behaviours related to information and security systems, especially as technological advancements like ICT have rapidly evolved over the last two decades. The ICT revolution has significantly impacted industries, economies, and organizational structures, fostering growth and enhancing productivity but also introducing new challenges in securing digital assets (Yang & Gu, 2021; Adeleye et al., 2022). Despite these advancements, particularly in Africa, the implementation of effective IS education is hindered by limited

resources and a shortage of skilled professionals. Efforts such as Nigeria's National Information Technology Development Agency (NITDA) cybersecurity initiatives and the inclusion of IS courses in university curricula aim to address these gaps (Dada, 2021). Awareness of information security is crucial to preventing cyber threats, with research showing that personal experiences with cyber incidents can increase awareness and adoption of security measures (Alotaibi, 2020; Renaud & Ophoff, 2021). However, studies highlight that despite heightened awareness, individuals often fail to act on security knowledge due to convenience, time constraints, or lack of training, and educational institutions face challenges in translating awareness into effective security practices (Kovačević & Radenković, 2020; Alharbi et al., 2021). Therefore, while raising awareness is essential, continued efforts are needed to ensure that security measures are implemented effectively (Chauhan, 2024; Das, 2019; Adeoye, Oluwole & Blessing, 2013).

Students' Information Security Awareness and Interest

A study explored Information Security Awareness (ISA) among university students, examining the impact of individual factors on ISA levels. Using a 30-item questionnaire with 614 students, Pearson's correlation coefficient was applied to analyze relationships between factors and perceived ISA levels. Results showed no significant correlation between age, nationality, discipline, and education level with ISA. However, gender and training had significant correlations with ISA, particularly in knowledge and behavior, while age and experience were correlated with ISA, and living area influenced knowledge. The study enhanced understanding of ISA among students (Farooq et al., 2015). Additionally, student interest in information security increases when real-world examples and culturally relevant content are used (Akande et al., 2024), and teaching strategies like gamification promote engagement (Okibe, 2024), fostering proactive digital citizenship in Africa (Ogunyemi, 2024).

Why CTCA – A Culturally Relevant Instructional Strategy?

After over forty years of research, the Culturo-Techno-Contextual Approach (CTCA) was developed to enhance science teaching in Africa (Okebukola et al., 2016). Unlike traditional lecture-based methods, CTCA adopts a learner-centered approach, engaging students as active participants. It integrates cultural, technological, and contextual factors, making learning more relevant and practical. By incorporating local contexts, such as objects and events within the school environment, CTCA moves away from abstract concepts and rote learning, fostering deeper understanding. This approach encourages student engagement, active knowledge exchange, and positive feedback, improving the overall educational experience (Oladejo et al., 2022; Akintoye et al., 2023; Adam et al., 2024b).

This innovation not only improves educational outcomes but also fosters a stronger sense of ownership over cybersecurity solutions. It empowers individuals

to adopt secure online practices that are tailored to their cultural environment, thus contributing to a safer digital space across the continent.

The following questions were raised to guide the investigation:

1. Will there be any difference in the (a) awareness, and (b) interest of students taught Information Security using the CTCA compared to those taught using the Conventional Lecture Method?
2. What are the students' perceptions of the impact of CTCA on their awareness and interest in Information Security?

The following null hypothesis (H0) were formulated from the research question above and tested at an alpha level of 0.05. $H0_1$: There will be no statistically significant difference in the awareness and interest of students taught information security using the CTCA and Conventional Lecture Method.

Theoretical, and Conceptual Frameworks Underpinnings the Study

The Culturo-Techno-Contextual Approach (CTCA) has been developed over more than forty years of research in Nigeria, formally introduced in 2015 as an additional teaching method for science education (Okebukola, 2020). CTCA combines cultural, technological, and geographic contexts to enhance teaching and learning. It integrates students' cultural backgrounds, the increasing use of technology in classrooms, and the unique characteristics of each school environment to make science lessons more relevant and practical (Adam et al., 2024a; Ademola et al., 2022). The study's conceptual framework focuses on integrating culturally relevant teaching with information security education, aiming to improve student engagement, awareness, and real-world application of security principles, fostering responsible digital behaviors (Okebukola, 2020).

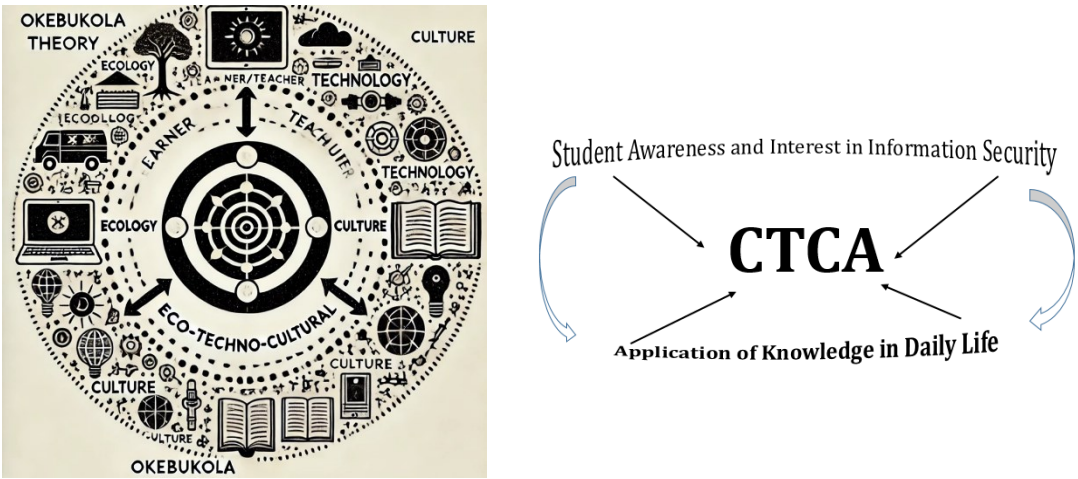

Figure 1. The CTCA Framework

From figure 1, The CTCA synthesises these various theories and philosophies to create a culturally relevant, socially interactive, and contextually grounded

approach to information security education. By harmonising classroom learning with cultural relevance, the approach not only fosters awareness of security principles but also sparks a deeper interest in exploring the complexities of the field. Students, through this model, can see themselves as active participants in shaping the future of information security within their own cultural and societal frameworks.

Context and Participants Details

This study aims to enhance Information Security (IS) awareness and interest among students across Ghana, Nigeria, and other African sub-regions, addressing the growing need for digital literacy. A total of 106 students from diverse educational backgrounds participated, with 50.95% in their final year and 49.05% in earlier stages. The gender distribution showed 60.38% females and 39.62% males, emphasizing the need for inclusive IS programs. Age-wise, 50.94% were between 10-15 years, and 49.05% between 15-20 years. Notably, 95.2% of participants had educated parents, suggesting supportive home environments to foster digital literacy (Okebukola et al., 2020). The study sample consists of 54 students from JHS '1' (50.94%) and 52 from JHS '2' (49.05%). More females (60.38%) than males (39.62%) participated, with ages split evenly between 10-15 years (50.95%) and 15-20 years (49.05%). Most participants (95.28%) have educated parents.

2. Methodology

Research Design

This study employed a mixed-method research design, using an explanatory sequential approach to combine quantitative and qualitative data for a comprehensive understanding of students' awareness and interest in Information Security (IS). Intact classroom groups were used to maintain natural dynamics. While the study focused on quantitative methods, in-depth interviews provided additional context, enriching the analysis and ensuring the reliability of findings.

Population of the Study

The study involved 106 Junior High School (JHS) ICT students from Mataheko '1' and '2'. The experimental group of 54 students was taught using the Computer-Assisted Teaching and Learning Approach (CTCA), while 52 control group students received traditional lectures. The sample included mixed-ability, mixed-gender students aged 11-20, using a multi-stage sampling method.

Instrumentation

The researcher developed two data collection instruments: the Students Information Security Awareness and Interest Questionnaire (SISAIQ) and the CTCA Perception Interview Guide (CPIG). SISAIQ collected quantitative data

through closed-ended and Likert-scale questions, measuring students' knowledge, attitudes, and motivation regarding information security. CPIG gathered qualitative data via open-ended questions exploring students' perceptions of the CTCA. Expert feedback from STEM Education scholars and a pilot test ensured the validity and reliability of both instruments for accurate data collection.

Procedure for Data Collection

This study utilized a mixed-method approach, collecting both quantitative and qualitative data. The quantitative phase began with a pretest to assess students' awareness and interest in information security, administered to both experimental and control groups. Following the pretest, the treatment phase involved two weeks of teaching, with 80-minute sessions. The experimental group was taught using the CTCA strategy, while the control group received traditional lectures. Qualitative data were gathered from five students in the experimental group.

Treatment Procedure of the CTCA in the Experimental Group

The implementation of CTCA in the experimental group followed the five steps in implementing CTCA in the classroom (Okebukola, 2020). Implementing CTCA involves featuring the culture, technology and context frameworks in the delivery of every lesson. It follows a 5-step process. These steps are:

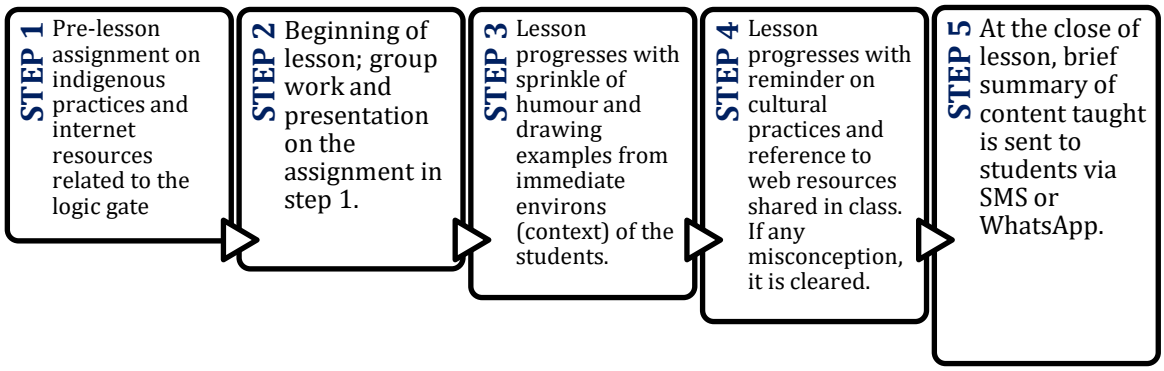

Figure 2. Implementation of the CTCA (Source Author 1)

Treatment Procedure of the CTCA in the Experimental Group

The implementation of CTCA in the experimental group followed a five-step process. Step 1: Students reflect on indigenous knowledge and search for online resources related to the lesson. Step 2: In groups, students share reflections on cultural knowledge and web-based ideas, with leaders presenting findings. Step 3: The teacher uses local examples to make lessons more tangible. Step 4: Indigenous knowledge is revisited to clarify misconceptions. Step 5: A lesson summary is sent via SMS/WhatsApp, or printed for those without mobile access.

Explanation of Indigenous knowledge and cultural practices related to information security

In many African societies, the talking drum serves as a potent channel of traditional communication. It is one of the most efficient communication methods used in villages and rural areas to enhance grassroots mobilization for societal development. The real significance of the talking drum lies in the role it plays in communication. In its earliest form, the talking drum served as an aid to ancient storytellers. These traveling poets and musicians would use the talking drums to carry on the oral traditions of their culture. Talking drums were used as a means of inter-village communication by themselves rather than any accompaniment.

Culture represents the way of life in a society, with the talking drum being vital in promoting cultural heritage, particularly in Tiv land and Sub-Saharan Africa. Beyond its use in social events and festivals, it serves as an essential communication tool for storytelling, conveying messages, and summoning ceremonial dances. The drum also plays a significant role in worship and imparting life lessons.

Symbols and Visual Codes

Adinkra Symbols (Ghana): These are visual symbols used by the Akan people of Ghana to communicate ideas, philosophies, or concepts. The symbols are often used on textiles, pottery, or walls, and each carries a specific meaning, aiding in conveying wisdom or important societal messages.

Nsibidi (Cross River, Nigeria): Nsibidi is a system of symbols used by the Efik, Ibibio, and other ethnic groups in southeastern Nigeria. It was historically used for communication, including keeping secrets or conveying messages in a way that only those with the knowledge of the symbols could interpret.

Information security protects data from unauthorized access while ensuring its availability and integrity. Similar to scarecrows deterring birds or shrines guarding valuables, security systems prevent unauthorized access. Just as only the chief priest can access the shrine, authorized individuals ensure that stored information is kept secure and remains unaltered when needed?

Implementation of the Lesson Using Lecture Method

Step 1: The teacher introduced "Information Security," linking it to students' prior knowledge. Step 2: The term was defined, and components were discussed. Step 3: Security strategies were explained. Step 4: Real-life examples of information security were provided. Step 5: The lesson was summarized. A post-test and questionnaire were then administered to both groups, with scores recorded.

After the post-test, seven students from the treatment group selected at random, comprising both sexes, were randomly selected for the qualitative phase of the study – interviews using the Information Security and CTCA Perception Interview Guide (ISCPIQ). The consent of the selected students was obtained before this session was coordinated. The interview took place in a conducive noise-free

atmosphere and lasted 45 minutes. Student responses were taken with a phone recorder, and salient points were taken on a notepad.

3. Results and Discussion

This study used a mixed-method approach to assess students' awareness and interest in information security. After obtaining permissions, a pretest was administered to both experimental and control groups. The treatment phase, lasting two weeks, involved the experimental group learning via the CTCA approach and the control group through traditional lectures. Afterward, qualitative data were collected to gain insights into students' perceptions, aiming to evaluate the effectiveness of CTCA in enhancing engagement with information security.

Reliability of Students Information Security Awareness

The reliability of the first part of the SISAIQ (Students Information Security Awareness) was tested using Cronbach's alpha. The instrument was administered to students in the pilot school. A Cronbach's alpha value of 0.7 or above was required to ensure the instrument's reliability.

Table 1. Reliability of Information Security Awareness

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.75	.76	20

The table 1 presents two values of Cronbach's Alpha for a set of 20 items. The first value, 0.75, represents Cronbach's Alpha based on the original data, while the second value, 0.76, is based on standardized items. Both values indicate a good level of internal consistency, with values above 0.71 generally considered acceptable for reliability testing. The 20 items suggest that the scale or instrument being tested has a moderate to good reliability.

Table 2. Reliability of Information Security Interest

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.71	.71	12

Table 2 shows the reliability statistics for a scale measuring Information Security Interest, based on 12 items. The Cronbach's Alpha value of 0.71, both for the original and standardized items, indicates acceptable internal consistency, as values above 0.7 are generally considered reliable. This suggests that the 12 items in the scale are measuring the intended construct with reasonable consistency.

Students Awareness in Information Security

The second research question investigated whether the CTCA influenced students' awareness of information security. The null hypothesis proposed no significant difference in awareness between students taught with CTCA and those taught via lectures. ANCOVA was employed to compare posttest scores, adjusting for pretest scores. Assumptions of normality and homogeneity of variance were verified using Kolmogorov-Smirnov, Shapiro-Wilk, and Levene's tests, with both groups meeting the normality requirement.

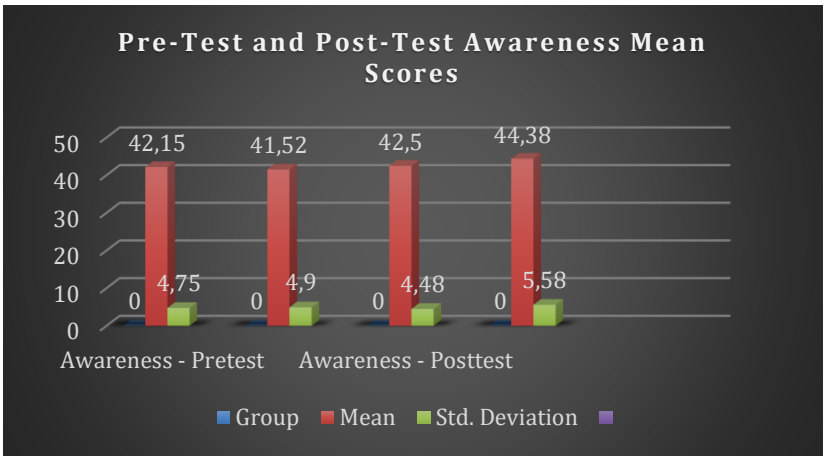

Figure 3. The Pre-Test and Post-Test Mean Scores for Awareness in Both Control and

Experimental Groups

Figure 2 shows the pre-test and post-test mean scores for awareness in both groups. The experimental group had a pre-test mean score of 42.15, while the control group had 41.52. After the treatment, the experimental group's post-test score increased slightly to 42.50, while the control group scored 44.38. ANCOVA analysis revealed a statistically significant difference, with the CTCA group showing better awareness [F (1, 103) = 3.91; p = .05], leading to the rejection of the null hypothesis.

Table 3. Analysis of Covariance (ANCOVA) on Awareness Post-Test Scores of Experimental and Control Groups with Pre-Test Scores as Covariate.

Dependent Variable: Awareness – Posttest						
Source	**Type III Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**	**Partial Eta Squared**
Corrected Model	116.60[a]	2.00	58.30	2.28	0.11	0.04
Intercept	2104.33	1.00	2104.33	82.44	0.00	0.45
Awareness - Pretest	22.51	1.00	22.51	0.88	0.35	0.01
GROUPS	99.83	1.00	99.83	3.91	0.05	0.04
Error	2629.30	103.00	25.53			
Total	202629.00	106.00				
Corrected Total	2745.90	105.00				
a. R Squared = .042 (Adjusted R Squared = .024)						

Table 3 presents ANCOVA results assessing the impact of experimental and control groups on post-test awareness scores, with pre-test scores as a covariate. The model explains 4.2% of the variance in post-test scores ($\eta^2 = 0.04$). The intercept term is highly significant ($p < 0.01$), indicating prior awareness influences post-test scores. The experimental group showed greater improvement ($F = 3.91$, $p = 0.05$), but the pre-test score had minimal impact ($\eta^2 = 0.01$). The total variance explained is modest, with adjusted R-squared at 0.024. Overall, the group effect on post-test awareness is small but statistically significant.

Students Security Information Security Awareness

The first research question was to determine if there is any difference in information security awareness between students taught using the CTCA method versus the lecture method. Analysis indicated that CTCA was more effective, with a significant difference in awareness [F (1, 103) = 3.91; p=.05]. The null hypothesis was rejected, showing that CTCA notably impacts students' information security awareness, with a moderate effect size of 4% (partial eta-squared = 0.04). Despite both groups having prior awareness, CTCA led to an increase in the experimental group's posttest scores. This suggests that while students have some awareness, their understanding is limited. Educational institutions should enhance information security training to equip students for the digital economy, especially as Africa embraces digital transformation.

Students Information Security Interest

Table 4. Pre-Test and Post-Test Interest Mean Scores for Experimental and Control Groups

	Groups	**Mean**	**N**	**Std. Deviation**
Interest - Pretest	Experimental	26.96	54	3.42
	Control	23.69	52	4.60
Interest - Posttest	Experimental	28.28	54	4.51
	Control	26.65	52	3.62

Table 4 shows the pre-test and post-test mean interest scores for both the experimental and control groups. For the pre-test, the experimental group had a mean score of 26.96 with a standard deviation of 3.42, while the control group had a mean of 23.69 with a standard deviation of 4.60. After the intervention, the experimental group's post-test mean score increased to 28.28 (SD = 4.51), while the control group's post-test mean score was 26.65 (SD = 3.62). These results suggest that both groups showed an increase in interest, but the experimental group had higher mean scores at both the pre-test and post-test.

Table 5 shows the results of an ANCOVA analyzing post-test interest scores for the experimental and control groups, with pre-test scores as a covariate. The model explains a small amount of variance in post-test interest ($R^2 = 0.04$). There is a marginally significant difference between groups ($F = 4.67$, $p = 0.03$), indicating the experimental group had greater interest. However, pre-test interest

scores did not significantly predict post-test scores (F = 0.54, p = 0.47). The intercept term is highly significant (p < 0.001), suggesting a baseline difference. The CTCA method led to significantly higher interest in information security compared to lectures (F = 4.67, p = 0.03), with a moderate effect size of 0.04.

Table 5. Analysis of Covariance (ANCOVA) on Interest Post-Test Scores of Experimental and Control Groups with Pre-Test Scores As Covariate

Tests of Between-Subjects Effects Dependent Variable: Interest – Posttest						
Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	78.897[a]	2	39.45	2.34	.10	.04
Intercept	2222.64	1	2222.64	131.91	.00	.56
Interest - Pretest	9.04	1	9.04	.54	.47	.01
GROUPS	78.76	1	78.76	4.67	.03	.04
Error	1735.57	103	16.85			
Total	81867.00	106				
Corrected Total	1814.46	105				
a. R Squared = .04 (Adjusted R Squared = .03)						

Perspectives of Students on the CTCA as a Teaching Method

The study also sought to collect students' views and perceptions on the use of the CTCA as an instructional method. The responses saw respondents highly advocating for the adoption of the CTCA as a teaching method as it helped them understand the topic of information security.

As reported by the interviewed respondents on the difficulties faced in learning ICT topics before the intervention of the CTCA, the students generally reported negative experiences. For instance,

Afriyie (Pseudo name), Female, and 16 years: *The notes are too long and not straight to the point. I always get bored reading more because of that. Also, the teachers couldn't use our surroundings or things around us to help explain things better.*

Sly (pseudo name), Male, and 17 years: *Before CTCA methods were used, ICT topics used to be very hard to understand because they came with long, complicated notes that made students feel bored and lazy to complete.*

Based on the feedback obtained from respondents, it is evident that the lecture method utilized by the teacher was perceived as complex and challenging to comprehend. The explanations provided were often abstract, accompanied by excessively lengthy notes, making the learning process difficult. These findings align with the research conducted by Okebukola et al. (2021) and Onowugbeda et al. (2022b), both of which identified a statistically significant difference between the CTCA approach and the traditional lecture method. This difference was attributed to the persistent challenge of conveying intricate concepts in the teaching and learning process. The consensus among these studies underscores the

importance of exploring alternative teaching methodologies, such as CTCA, to overcome barriers and enhance the effectiveness of the learning experience.

The views of respondents were again solicited on their respective perceptions of the CTCA in learning ICT, and they gave their views. They revealed the following:

Sandra (pseudo name), Female, 15 years: *The CTCA method used by the teacher is good because instead of long notes, they send us shorter versions. This helps us understand the topics better.*

Nana Kwame (pseudo name), Male, 15 years: *The CTCA method has helped me in my studies because I don't have to spend a lot of time reading my notes. The topics are already explained in a way that I can easily understand.*

According to feedback from interviewed students, the preference for the CTCA method was attributed to the use of concise and summarized notes, focusing on key aspects of the topic. This approach resonated with the students, as it eliminated the need for extensive reading and allowed them to concentrate on crucial concepts. The students reported an increased interest in ICT classes, attributing this positive shift to the avoidance of cramming short notes, which had been a consequence of the traditional lecture method. This finding aligns with the idea that learning should be meaningful rather than based on rote memorization, as advocated by Okebukola (2020), highlighting the advantages of the CTCA method in promoting a deeper understanding of the subject matter.

The students interviewed also revealed the aspects of the CTCA they enjoyed. The responses of the students revealed the following:

Abena (pseudo name) Female, 16 years: *I liked the example with our school environment, especially the example with the school's gate and the security man as a means of protecting the contents and people in the school from unauthorized people.*

Sly (pseudo name), Male, 17 years: *I liked the assignment that involved indigenous knowledge. Using cultural and indigenous knowledge helped us connect ICT topics to things we see every day, making it easier for me to understand the topic.*

Nana Kwame (pseudo name), Male, 15 years*: I liked watching YouTube videos on the topic. My dad watched it with me and explained some parts to me.*

Feedback from interviewed students highlights that the CTCA method, which integrates cultural and indigenous knowledge, made lessons simpler and more accessible compared to conventional lectures. Students found this approach eliminated the need for lengthy notes, increased their interest in ICT classes, and improved academic performance by adapting topics to their understanding. The CTCA method's effectiveness lies in its combination of cultural context, technology, and the school's location. This approach helps students relate difficult concepts to their indigenous knowledge, enhancing meaningful learning and academic achievement. These findings align with previous research showing the CTCA method's positive impact on student performance.

1. Discussion of Findings

The research problem was introduced in the previous chapters, followed by a review of the literature and an explanation of the methodology a quick look at the responses shows consistency between the quantitative and qualitative aspects, likely due to effective data collection methods. This underscores the benefits of the mixed methods research design, combining both types of data for a more comprehensive understanding of the problem. Each objective is discussed concerning relevant literature, providing interpretations alongside the results.

Students Information Security Awareness

Research Question 1a: Is there a statistically significant difference in the awareness of students taught Information Security using the CTCA and the lecture method?

Null Hypothesis (Ho1): There will be no statistically significant difference in the awareness and interest of students taught Information Security using the CTCA and Conventional Lecture Methods.

Finding*:* Results of the mean analysis and ancova skewed in favour of CTCA as an effective mode of teaching over the lecture method. The study found a statistically significant difference in the awareness of students taught using the CTCA compared to those taught using the lecture method in information security [F (1, 103) = 3.91; p=.05].

Decision*:* Based on the result, the null hypothesis that there will be no statistically significant difference in the awareness of information security between students taught using the CTCA and those taught using the lecture method was rejected.

The study found that the CTCA significantly influences students' awareness of information security, with a moderate effect size of around 4%. This is due to the influence of both treatment groups and pre-treatment scores, with a partial eta-squared value of 0.04. This suggests that CTCA has a significant impact on students' awareness of information security. Aside from the significance of the study, it was also observed that students both from the experimental and control groups had prior knowledge and some level of awareness of information security, as evident in their mean scores (42.15 and 41.52) respectively for pretest and (42.50 and 44.38) respectively for posttest. Even though the control group had a higher mean, the experimental group saw an increase in their mean after the treatment, indicating that the CTCA had an equal impact on their awareness.

Discussion*:* Moletsane, & Tsibolane, (2020,) identified a knowledge deficit and lack of awareness among students in information security, particularly in the domain of mobile security. The study underscored the necessity for enhanced education and training to ensure students possess adequate knowledge of information security, even when some prior knowledge exists. Similarly, Aldarmaki, (2018) identified cultural factors influencing information security awareness, contributing to students' pre-existing awareness of information security concepts. The study emphasized the significant role of the human component, encompassing both knowledge and behaviour, in ensuring ICT security. Cultural influences were recognized as factors shaping individuals'

security knowledge and behaviour, with varying levels of security awareness attributed to cultural variations. This insight highlights the interconnectedness of cultural factors and information security awareness, emphasizing the importance of addressing both technical and cultural aspects in comprehensive information security education.

The research findings suggest that while students demonstrate a certain degree of awareness regarding information security, their understanding of the associated concepts appears limited. Factors influencing the level of students' information security awareness include their education level, previous technology experience, and training. It is recommended that educational institutions prioritize providing students with comprehensive training and education on information security, concurrently advocating for the adoption of best practices to safeguard their digital identities. As Africa undergoes a digital revolution, it becomes crucial to ensure that students have access to essential resources and opportunities for acquiring the skills and knowledge necessary to excel in the digital economy.

Students Information Security Interest

Research Question 1b: Is there a statistically significant difference in the interest of students taught Information Security using the CTCA and the lecture method?
Finding*:* Results of the mean analysis and ancova skewed in favour of CTCA as an effective mode of teaching over the lecture method. The study found a statistically significant difference in the awareness of students taught using the CTCA compared to those taught using the lecture method in information security [F (1, 103) = 4067; p=.03].
Decision*:* Based on the result, the null hypothesis that there will be no statistically significant difference in the interest in information security between students taught using the CTCA and those taught using the lecture method was rejected.

The study found that the CTCA significantly influences students' interest in learning information security, with a moderate effect size of around 4%. This is due to the influence of both treatment groups and pre-treatment scores, with a partial eta-squared value of 0.04. This suggests that CTCA has a significant impact on students' interest in information security. It was observed from the study that both the experimental and control groups were very much interested in information security as a topic and a possible career path in the future. The interest of these students in information could be linked to their pre-lesson assignments on watching YouTube videos on information security and its possible harm if not strictly adhered to.

Discussion*:* In a comprehensive examination, Taha, & Dahabiyeh, (2021) compared students' information security behaviours across the use of both cell phones and computers. The outcomes revealed a commendable positive inclination among students towards information security. This suggests a genuine interest in grasping the significance of maintaining a secure online presence to thwart potential exploitation. Furthermore, the research conducted by Ahmead, et al., (2024) reinforced these findings. It unveiled that students actively

implemented robust protective measures, showcasing proficiency in areas such as computer knowledge, mobile computing, data loss prevention, encryption practices, and managing online social media networking securely. This collective evidence portrays a proactive stance among students, indicating a strong commitment to safeguarding their digital assets and navigating online interactions responsibly.

The findings on students' interest in information security still point to the direction of training and education on issues of information security in such a manner that will draw more young ones into that knowledge space. This finding highlights an important development and emphasises the need for interventions to bridge the information security interest gap and encourage students to translate their knowledge into action. Furthermore, the findings of the studies on students' behaviors and attitudes towards information security align with the growing emphasis on ICT education in Sub-Saharan African countries. For students in countries like Ghana and Nigeria, there is a clear interest in the subject, but there are challenges related to infrastructure, curriculum, and practical training that need to be addressed to ensure these students perform well in ICT subjects and transition into capable professionals in the digital world. Addressing these barriers could enhance both the academic performance of students and their ability to contribute to the growing digital economy in Africa.

4. Conclusion

The study draws its conclusions from the synthesis of both qualitative and quantitative findings. In the quantitative phase, students in the experimental group CTCA demonstrated superior academic performance compared to their counterparts in the control group (lecture method). Regarding awareness of information security, students generally exhibited a fair understanding of basic awareness tips, with the control group indicating a higher mean than the experimental group. However, after the implementation of CTCA, the experimental group experienced an increase in their awareness level. Furthermore, the experimental group displayed a higher level of interest in information security compared to the control group. These quantitative results contribute to the overall conclusion regarding the efficacy of the Culturo-Techno-Contextual Approach in positively impacting students' academic performance, awareness, and interest in information security.

In the qualitative phase, the thematic analysis revealed a notably positive preference for the Culturo-Techno-Contextual Approach (CTCA) and a high level of student satisfaction with this instructional method. Consequently, the study concludes that CTCA, particularly in the realm of information security, should be effectively and sufficiently employed to attain meaningful learning outcomes. The approach has demonstrated its potential to improve students' academic achievement, elevate awareness and interest levels in information security, and serve as a motivating factor for students to engage in learning by overcoming barriers and difficulties. The qualitative findings further reinforce the overall

efficacy of CTCA as a pedagogical approach with positive implications for students' learning experiences and outcomes.

References

Adam, U. A., Okebukola, P. A., & Oladejo, A. I. (2021). Exploring the Efficacy of the Culturo-Techno-Contextual Approach (CTCA) in Improving Academic Achievement of Secondary School Students in Genetics. Proceedings of the Faculty of Education Annual Conference, Lagos, Nigeria

Adam, U. A., Lameed, S. N., Owolabi, T., Onowugbeda, F. U., Oladejo, A. I., Okebukola, P. A., & Mustapha, G. A. (2024a). The potency of culture, technology, and context in a biology classroom: Culturo-Techno-Contextual Approach in action. International Journal of Science Education, 1-26.https://doi.org/10.1080/09500693.2024.2405667

Adam, U. A., Onowugbeda, F. U., Islami, N., & Ogolo, K. G. (2024b). Testing the potency of ethnoscience instruction on biology students' critical thinking ability. The Journal of Educational Research, 1-10.

Adeleye, B. N., Jamal, A., Adam, L. S., & Oyedepo, T. (2022). ICT leapfrogging and economic growth among SAARC economies: Evidence from method of moment's quantile regression. Journal of Global Information Technology Management, 25(3), 230-253.

Ademola, I., Okebukola, P. A., Oladejo, A. I., Gbeleyi, O., Onawugbeda, F., Awaah, F., & Peter, E. (2022, March). Improving the Achievement of Secondary School Students: How can CTCA help in Ecology? In Presented at the 95th Annual Conference of NARST.

Adeoye, Y. M., Oluwole, A. F., & Blessing, L. A. (2013). Appraising the Role of Information Communication Technology (ICT) as a Change Agent for Higher Education in Nigeria. International Journal of Educational Administration and Policy Studies, 5(8), 177-183.

Adeshola, I., & Oluwajana, D. I. (2024). Assessing cybersecurity awareness among university students: implications for educational interventions. Journal of Computers in Education, 1-23.

Adisa, O. T. (2023). The impact of cybercrime and cybersecurity on Nigeria's national security.

Ahmead, M., El Sharif, N., & Abuiram, I. (2024). Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: a cross sectional study. Crime Science, 13(1), 29.

Akande, A., Coker, D. C., & Pinto, J. F. (2024). The Constructs of Leadership and Politics: Theory to Praxis. In Leadership and Politics: New Perspectives in Business, Government and Society (pp. 1-35). Cham: Springer Nature Switzerland.

Akintoye, H., Adam, U. A., Lameed, S. N., Bankole, I. S., & Ayodeji, B. (2023). A case for culturo-techno-contextual approach for enhanced academic achievement in STEM education. Journal of Educational Sciences, 7(4), 530-544.

Aldarmaki, A. R. (2018). Customization of School-Based Cyber Security Awareness Material for grade 12 Emirati Students (Doctoral dissertation, Khalifa University of Science).

Alotaibi, F. G. S. (2020). A Novel Framework for Improving Cyber Security Management and Awareness for Home Users (Doctoral dissertation, University of Plymouth).

Aparisi, D., Delgado, B., & Bo, R. M. (2024). Explanatory model of cyberbullying, cybervictimisation, aggressiveness, social anxiety, and adaptation to university: a structural equation analysis. Journal of Computers in Education, 1-22.

Awe, I. B., & Ewata, T. O. (2020). ICT Psychomotor Teaching Strategy in Oral English Class in Akure, Nigeria. An interdisciplinary quarterly from the north, 124.

Chauhan, V. (2024). Understanding users' protective behavior and its suppressor effect on the perceived risk in M-wallet/banking use: An Indian urban-rural comparison. Technological Forecasting and Social Change, 201, 123255.

Dada, A. (2021). Digital Entrepreneurial Behaviour of Millennials in the Fourth Industrial Revolution in Southwest Nigeria: Digital Entrepreneurial Behaviour of Millennials. African Journal of Science Policy and Innovation Management, 2(1&2), 41-60.

Das, K. (2019). Role of ICT for better mathematics teaching. Shanlax International Journal of Education, 7(4), 19-28.

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015, August). Information security awareness in educational institution: An analysis of students' individual factors. In 2015 IEEE Trustcom/bigdataSE/ispa (Vol. 1, pp. 352-359). IEEE.

Jones, L. A. (2024). Unveiling Human Factors: Aligning Facets of Cybersecurity Leadership, Insider Threats, and Arsonist Attributes to Reduce Cyber Risk. Socioeconomic Challenges, 8(2), 44-63.

Kovačević, A., & Radenković, S. D. (2020). SAWIT—security awareness improvement tool in the workplace. Applied Sciences, 10(9), 3065.

Moletsane, T., & Tsibolane, P. (2020, March). Mobile information security awareness among students in higher education: An exploratory study. In 2020 conference on information communications technology and society (ICTAS) (pp. 1-6). IEEE.

Ogunyemi, A. A. (2024). Cyber Risks and the Nigerian Business Sector: A Critical Analysis of the Emerging Cyber Insurance Market in Nigeria. ACU Journal of Social Sciences, 3(1).

Okibe, E. S. (2024). An Exploratory Analysis of the Efficacy of Nigeria's Cybercrime (Prohibition, Prevention, Etc.) Act 2015: Legal Frameworks, Challenges, and Prospects for Combating Cybercrime. Alex-Ekwueme Federal University Faculty of Law Ll. B Projects.

Oladejo, A., Akinola, V., Ebisin, A., & Olateju, T. T. (2022). Culturally Relevant Pedagogies in Enhancing Students Learning of ICT Concepts: A Test of the Efficacy of CTCA. West African Journal of Open & Flexible Learning, 11(1).

Oliveira, K. K. D. S., & De Souza, R. A. (2022). Digital transformation towards education 4.0. Informatics in Education, 21(2), 283-309.

Renaud, K., & Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. Organizational Cybersecurity Journal: Practice, Process and People, 1(1), 24-46.

Roosman, H. S. (2022). Information Systems Security Countermeasures: An Assessment of Older Workers in Indonesian Small and Medium-Sized Businesses (Doctoral dissertation, Nova Southeastern University).

Taha, N., & Dahabiyeh, L. (2021). College student's information security awareness: a comparison between smartphones and computers. Education and Information Technologies, 26(2), 1721-1736.

Yagboyaju, D. A. (2023). The Implication of Corruption to Nigeria's Internal Security: Insights from Selected Security Agencies. Scientia Militaria: South African Journal of Military Studies, 51(1), 129-150.

Yang, F., & Gu, S. (2021). Industry 4.0, a revolution that requires technology and national strategies. Complex & Intelligent Systems, 7, 1311-1325.

How to cite this article:

Gbeleyi, O. A., Foli, J. Y., Akintolure, S. O., Oladejo, A. I., & Ariyibi, O. O. (2025). Enhancing Students' Awareness and Interest in Information Security: The Role of Culturally Relevant Instructional Strategy. *Journal of Educational Sciences*, *9(1)*, 288-304.