MULTIDISCIPLINARY SCIENCE JOURNAL

RESEARCH ARTICLE
Published Online: June 16, 2026
https://doi.org/10.31893/multiscience.2026807

Effectiveness of whatsapp learning platform in preventing cybercrime in higher institutions

Matthew Omojemite[a]

[a]Continuing Professional Teacher Development, Faculty of Education, Walter Sisulu University, South Africa.

Abstract The purpose of this study was to examine the effectiveness of WhatsApp learning platforms in preventing cybercrime among students in higher institutions in Ekiti State, Nigeria. The study aimed to assess students' awareness of cybercrime threats, determine the effectiveness of WhatsApp in enhancing knowledge of cybersecurity practices, evaluate its influence on students' attitudes and behaviours, and identify challenges associated with its use. A descriptive survey research design was employed. The population comprised all students in selected higher institutions in Ekiti State, from which a sample of 400 students was drawn using stratified random sampling. Data were collected through a structured questionnaire, which was validated by experts and tested for reliability using Cronbach's alpha, yielding a reliability coefficient of 0.82. The instrument was administered directly to respondents, and the collected data were analysed using descriptive statistics and regression analysis. The findings revealed that students' awareness of cybercrime threats was generally moderate, while WhatsApp was effective in enhancing knowledge and positively influencing attitudes and behaviours toward safe online practices. However, challenges such as poor internet connectivity, distractions from non-academic content, limited participation, and technical difficulties were reported, affecting the platform's overall effectiveness. Regression analysis revealed that these challenges had a significant impact on both awareness and knowledge outcomes. Based on these findings, the study concluded that WhatsApp is a valuable tool for cybercrime prevention education, but its impact can be maximized by addressing infrastructural and operational constraints. Recommendations include improving internet access, providing technical support, training students on effective use of WhatsApp, and integrating cybersecurity education into the formal curriculum.

Keywords: awareness, cybercrime, cybersecurity, knowledge, prevention, Whatsapp platform

1. Introduction

Cybercrime has become a huge international menace and education systems have suffered a lot. According to recent estimates, the global cybercrime cost is estimated at approximately 9.5 trillion in 2024, and annual data provided by the Internet Crime Complaint Center of the FBI indicates that phishing and victim online fraud have significantly increased the number of reported cases in 2024 (Reuters, 2024; Higher Ed Dive, 2024). Ransomware and data breaches are a major cause of concern in the education sector. It has been reported that close to a half of higher education systems that are targeted by a ransomware experience massive destruction, causing disruption in operations, exposure of sensitive information and expensive recovery process (Sophos News, 2023; eSentire, 2024). Colleges and universities are the best targets as they have huge amounts of sensitive data such as student records and research output which are often run on open and diverse networks which are hard to secure. A case in point is the infamous breach of the University of the West of Scotland that happened in 2024 and resulted in the leakage of hundreds of gigabytes of data, leading to the reputational and financial losses (The Times, 2024). In Africa, the law enforcing agencies have also been forced to react to the escalating magnitude of frauds that are facilitated by the Internet. As revealed by the Operation Serengeti of INTERPOL, the area is highly susceptible to cybercrime since the majority of cases involved business-email compromises, online scams, and digital extortion (AP News, 2024).

The students are one of the most vulnerable populations due to their excessive dependence on the internet and social media in their academic, social, and personal life. This can easily identify them as victims of phishing, identity theft, and hacking, as well as online fraud and cyberbullying. Nigeria and other researchers have found that most of students become victims of phishing because of their ignorance and bad online practices, and some become victims of identity theft or financial fraud (IIETA, 2022). The problem of cyberbullying is also prominent in the Nigerian universities, where trolling, outing, and online harassment are the main forms of this bullying which frequently leads to psychological stress and disengagement with studying (Cyberbullying Research Center, 2023). Notwithstanding these threats, studies have been carried out to reveal that a good number of students in higher institutions in Nigeria have low to medium awareness of cybersecurity. The results of controlled phishing experiments indicate that a significant proportion of students continue to fall into a trap of malicious links or provide

 Received: December 9, 2025 | Accepted: March 12, 2026

their credentials, and surveys also point to the lack of knowledge about preventive measures (E-Palli, 2022). Such findings will infer that cybersecurity training in most organizations is substandard and that it needs to undergo organized, curriculum-driven interventions. In this regard, the platforms which the students are already using on a routine basis to communicate and learn with provide a potential of cybersecurity education. An example is WhatsApp which is among the most popular applications used by undergraduates in Nigeria to discuss in groups, coordinate, and learn with their peers. Using WhatsApp in prevention education about cybercrime, thus, offers a viable and interactive means of enhancing awareness, attitudes, and risky Internet behavior change among higher institution students.

The aspect of cybersecurity education has been a paramount part of higher education in the world. Universities and colleges are the most obvious victims of cyberattacks since they possess a great deal of sensitive information such as student records and research. With the growing use of digital learning platforms by more institutions, the latter become susceptible to threats, including phishing, ransomware, and data breaches. Providing students with structured cybersecurity education helps them recognize and respond to cyber threats, reducing both personal and institutional risks. It is necessary to provide students with knowledge, skills and attitudes required to engage in safe online behavior. Research shows that students that are trained on cybersecurity can protect their accounts better, detect suspicious behavior on the Internet, and take preventive actions, including use of strong passwords and two-factor authentication (IIETA, 2022). Conventional classroom learning, however, is usually unable to keep up with the pace of cyber threats. Traditional lectures could focus on theory, neglecting the practice, and students would not be ready to attack in real life (ThriveDX, 2024). Also, the lack of time, inadequate resources, and student engagement can be considered among the factors that inhibit the efficiency of conventional teaching strategies (E-Palli, 2022). Due to these restrictions, teachers are looking into digital platforms and social media tools as the other means of imparting cybersecurity education. Applications such as WhatsApp that students already use to organize the academic process and collaborate with each other offer an interactive and somewhat flexible method of strengthening cybersecurity knowledge. Research indicates that learning can be incorporated into the regular communication tools to enhance the interaction and help students learn better about safe internet culture. Using these platforms will allow the higher institutions to go beyond classroom learning, and students learn to stay safe in the online world by putting into practice the habits and skills that they can apply.

The technology in social media has emerged as a significant medium in the education sector, since they are readily available, interactive and are common with students. According to their ability to communicate in real time, share resources fast and collaborate with peers, their popularity is based on making the process of learning flexible and engaging. Recent papers emphasize the effectiveness of WhatsApp as a learning tool. Abbasian (2024) conducted a study where training was conducted on WhatsApp, and the results showed improvement in the health ambassadors' knowledge about minor illnesses. In the same way, a study conducted by Mutair (2025) evaluated the effect of education on undergraduate nursing students on their level of performance and satisfaction through WhatsApp. These research show that WhatsApp has relevance in aiding the sharing of knowledge and peer learning. According to study by Greeff (2024), WhatsApp is also used by most students in their academic activities. They can easily navigate and access learning resources and are useful in interacting with other learners and teachers. Students said that WhatsApp helps with group learning and enables them to clarify their questions with ease. The availability and interactivity of the WhatsApps with a wide dissemination among students make it a useful resource in education as an educational tool that facilitates sharing of knowledge, peer learning, and behavior change.

The high institutions students are already on WhatsApp in large numbers both academically and socially. This is what renders WhatsApp a viable and cost-efficient tool in conveying cybercrime awareness and prevention education by virtue of this familiarity. Since students use the platform on a regular basis, implementing cybersecurity lessons within WhatsApp groups can enable institutions to go through the students, making them more engaged and active (Mutair, 2025; Greeff, 2024). Interactive and collaborative learning is also supported in WhatsApp. Students will be able to discuss in real time, chat in groups, share learning sources, and collaborate on tasks, which also contributes to the knowledge of the dangers of cybercrime and responsible Internet conduct. The studies indicate that WhatsApp learning can enhance knowledge retention, collaboration, positively impacting attitudes, and behavior (Abbasian, 2024; Mutair, 2025). With the help of a platform that students already use on a daily basis, higher institutions will be able to offer twenty-four-seven learning that is peer-assisted, which will prompt students to implement preventive steps to phishing, online fraud, identity theft, and other types of cyber-attacks. This strategy renders cybercrime education more practical, available and most likely to lead to a valuable behavior change.

WhatsApp is a popular learning and academic collaboration tool that has been studied and its role in enhancing knowledge, facilitating peer learning, and enhancing student engagement has been demonstrated (Mutair, 2025; Greeff, 2024). Nevertheless, limited studies have investigated its application in the prevention of cybercrime among learners in the institutions of higher learning. The existing literature is dedicated to the overall results of education and fails to address the impact of WhatsApp on cybersecurity knowledge and attitudes of students, as well as their online behaviour. This gap indicates that research in the form of WhatsApp as a cybercrime awareness and prevention platform is needed. Researching its usefulness in the field would assist institutions of higher learning to develop realistic and feasible techniques to impart into the

students the knowledge and habits that would keep them safe on the internet. The current research intends to fill this gap by looking at the success of WhatsApp learning platforms in facilitating cybercrime prevention among students.

1.1. Objectives of the Study

The core aim of the study is to analyze whether the WhatsApp learning platform is effective in ensuring that students in the higher institutions are promoted to prevent cybercrime. In particular, the research will evaluate the degree of cybercrime threat awareness among students by using the WhatsApp learning platform. As well, it seeks to look at the effectiveness of the platform in terms of improving the knowledge of cybersecurity practices among students. Moreover, the research will aim at establishing how much the WhatsApp learning platform affects the attitudes and behaviour of students in regards to cybercrime prevention. Lastly, the research will attempt to determine the issues surrounding the application of the WhatsApp learning platform in the education of cybercrime prevention in higher institutions.

1.2. Theoretical Framework

This study is grounded on the Social Learning Theory and the Technology Acceptance Model which, in combination with each other, presents a robust conceptual framework to the way digital tools like WhatsApp can affect learning outcomes and behavioural change among students.

1.2.1. Social Learning Theory

The Social Learning Theory, which is a propounding theory presented by Albert Bandura, elucidates that people acquire behaviour by observing, imitating and interrelating with their surroundings (Bandura, 1977; Bandura, 1986). The theory was formulated as an expansion of the traditional behaviourist learning theories by underlining the importance of the cognitive processes in the learning process. This theory was proposed by Bandura who proved that people only do not learn directly through reinforcement but also observe other people and the outcomes of their actions. The theory was postulated to describe the effects of social environments on the development of behaviour particularly through the use of modelling and vicarious reinforcement (Bandura, 1986).

The Social Learning Theory is premised on a few assumptions. First, learning is possible through observation of the behaviour of other people and its consequences. Second, people tend to emulate actions taken by reputable, esteemed or similar role models. Third, attention, retention, reproduction, and motivation are cognitive processes that are involved in the learning process (Schunk, 2012). Fourth, there is interaction between behaviour, personal factors, and environmental influences in a concept referred to as reciprocal determinism (Bandura, 1986). These suppositions emphasize the relevance of the social environment and exposure to the environment in the formation of behaviour.

The social learning theory offers a good explanation on how the students learn the cybercrime prevention behaviours using WhatsApp learning platforms. Group discussions, cybersecurity information sharing, and peer interaction through which students share and observe safe online behavior of colleagues and instructors would enable them to emulate the same. As an illustration, students can be taught not to click on phishing links, have a strong password, and report suspicious messages by watching others do so. This is consistent with the studies that have found that collaborative learning, built through social media, has the potential to improve knowledge sharing and behavioural change (Chaka et al., 2020; Chib et al., 2021). Thus, the theory justifies the application of WhatsApp as the social learning tool to enhance cybersecurity awareness, knowledge acquisition, and safe online behaviour in higher education students.

1.2.2. Technology Acceptance Model

Fred Davis developed the Technology Acceptance Model (TAM) in 1989 in order to demonstrate how users accept and adopt new technologies. The model was designed to assist predict the user behaviour concerning technology adoption, especially on information system and learning digital environments. TAM is also a product of previous behavioural theories and as such it was based on the theory of reasoned Action but developed to explain why individuals endorse or decline technological inventions upon the basis of their perceptions of usefulness and ease of use (Davis, 1989).

The Technology Acceptance Model has a few assumptions. One, perceived usefulness has a role in technology adoption, i.e. when the users perceive that the technology will enhance their performance or learning performance, they tend to adopt the technology. Second, the perceived ease of use has an impact on the adoption decision where users tend to use a technology that is easy and convenient to use. Third, behavioural intention is a good predictor of real behaviour of technology use (Davis, 1989; Venkatesh and Davis, 2000). The model further supposes that the perceptions of technology usefulness and usability can be influenced by external factors like social influence, infrastructure and user experience.

This study relies on TAM to explain how students will accept and use WhatsApp as a learning platform in cybercrime prevention learning. There is a risk that students would find cybersecurity learning with the help of WhatsApp more meaningful when they believe that the platform is helpful in enhancing their experience in cyber threats and when the platform seemed convenient to respond to communicative and learning processes. The ease of access and the capabilities of the platform to

send and receive messages real-time and collaborate in groups make the platform seem more useful to encourage awareness of cybersecurity. It is in line with the studies that mobile messaging platforms enhance student interaction and knowledge exchange and academic teamwork within higher education institutions (Mutair, 2025; Lee et al., 2023). TAM contributes to the argument that a positive perception of digital learning tools can change the attitude and behaviours of students in preventing cybercrime. Students will be more respectful of engaging in cybersecurity awareness communication by considering WhatsApp-based learning as helpful and convenient, which make them more likely to engage in online communication actively and use safer online practices.

1.3. Conceptual Framework

The conceptual framework shows how the study combines the Social Learning Theory (Bandura, 1977) and the Technology Acceptance Model (Davis, 1989) in the research to determine the effectiveness of the WhatsApp learning platform in enhancing cybersecurity-related awareness and prevention among students in higher institutions. The framework, as summarized in Figure 1, places WhatsApp as the focal point of learning that facilitates the acquisition of knowledge, peer interaction, and behavioral change as a representation of the principles of Social Learning Theory, which opposes the idea that a person learns through observation, imitation and social interactions. At the same time, the Technology Acceptance Model is used to describe how students adopt WhatsApp and maintain its use by the perceived usefulness of the platform and its perception of ease of use to influence the engagement and learning outcomesThose theoretical backgrounds are associated with the study aims: an increase in cybercrime awareness (Objective 1), an increase in cybersecurity knowledge, the development of attitudes and preventive behaviors among s students, and the establishment of barriers to the use of WhatsApp as a tool of cybercrime prevention (Objective 4). The two strategies used in conjunction provide a clear picture of the conceptual map of how WhatsApp facilitates digital learning and behavior change in cybersecurity education.

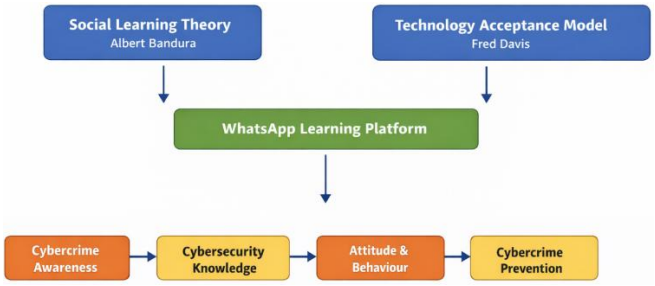

Figure 1 Conceptual Framework Linking the Theories to the Study Objectives.

1.4. Research Questions

What is the level of awareness of cybercrime threats among students in higher institutions through the use of WhatsApp learning platform?

How effective are WhatsApp learning platforms in enhancing students' knowledge of cybersecurity practices?

To what extent do WhatsApp learning platform influence students' attitudes and behaviors toward cybercrime prevention?

What challenges are associated with the use of WhatsApp learning platform for cybercrime prevention education in higher institutions?

1.5. Research Hypotheses

The challenges associated with the use of WhatsApp learning platform will not significantly predict the level of awareness of cybercrime threats among students in higher institutions.

The challenges associated with the use of WhatsApp learning platform will not significantly predict the effectiveness of WhatsApp learning platform in enhancing students' knowledge of cybersecurity practices.

2. Materials and Methods

2.1. Research Design

This study adopted a quantitative research design and employed a descriptive survey approach to examine the effectiveness of WhatsApp in promoting cybercrime awareness among students in higher institutions. Data were collected using structured questionnaires administered to a representative sample of students, which allowed for standardised measurement of their experiences, engagement, and knowledge of cybercrime prevention. This design enabled the researcher to analyse trends, patterns, and relationships between students' use of WhatsApp and their cybersecurity knowledge, attitudes, and behaviours.

2.2. Population

The population for this study comprised all undergraduate students enrolled in higher institutions in Ekiti State, Nigeria. This included approximately 35,000 – 39,999 students at Ekiti State University (EKSU), 43,000 students at Federal University Oye-Ekiti (FUOYE), and 8,500 students at Afe Babalola University (ABUAD). These students were selected because they actively use WhatsApp for academic and social purposes, making them suitable for assessing the platform's effectiveness in promoting cybercrime awareness and prevention. The population included both male and female students across various faculties and levels of study, providing a comprehensive perspective on how WhatsApp influences students' knowledge, attitudes, and online behaviours.

2.3. Sample and Sampling Technique

A sample of 400 undergraduate students was selected from the total population of students in higher institutions in Ekiti State, Nigeria. The stratified random sampling technique was employed to ensure representation across the three institutions Ekiti State University, Federal University Oye-Ekiti, and Afe Babalola University as well as across faculties, levels of study, and gender. This method ensured that the sample reflected the diversity of the population, allowing for more reliable and generalisable findings regarding the effectiveness of WhatsApp in promoting cybercrime awareness and prevention among students.

2.4. Research Instrument

The study utilized the "WhatsApp Cybercrime Awareness and Prevention Questionnaire (WCAPQ)" as the primary instrument for data collection. The WCAPQ was developed to measure students' awareness of cybercrime threats, cybersecurity knowledge, preventive attitudes and behaviours, and challenges associated with the use of WhatsApp learning platforms. The instrument was divided into four major subscales to improve construct validity and provide clearer measurement of study variables. The first subscale measured cybercrime awareness, with sample items such as "I am aware of common cybercrime threats such as phishing and online fraud." The second subscale assessed cybersecurity knowledge using items such as "WhatsApp learning materials help me understand how to protect my online accounts." The third subscale measured preventive attitudes and behaviours, with items such as "I regularly update my passwords to secure my online accounts." The fourth subscale examined challenges associated with WhatsApp learning, with items such as "Poor internet connectivity affects my participation in WhatsApp learning activities." The questionnaire was structured on a five-point Likert scale ranging from Strongly Disagree (1) to Strongly Agree (5), allowing respondents to indicate their level of agreement with each statement. This detailed description of the instrument strengthens transparency, improves construct measurement, and enhances the methodological rigor of the study.

2.5. Validity of the Instrument

The validity of the WhatsApp Cybercrime Awareness and Prevention Questionnaire (WCAPQ) was ensured through content and face validation. Experts in cybercrime, educational technology, and research methodology reviewed the instrument to confirm that the items adequately measured students' knowledge, attitudes, and preventive behaviours related to cybercrime. Their feedback was used to revise unclear or ambiguous items, ensuring the questions were relevant, precise, and aligned with the objectives of the study. This process strengthened the content validity of the instrument and ensured that it effectively captured the constructs under investigation.

2.6. Reliability of the Instrument

The reliability of the WhatsApp Cybercrime Awareness and Prevention Questionnaire (WCAPQ) was established through a pilot study conducted with 30 students from a higher institution outside the main study sample. The data collected were analysed using Cronbach's alpha coefficient, which yielded a value of 0.82, indicating good internal consistency. This demonstrated that the instrument was reliable for measuring students' use of WhatsApp, their cybersecurity knowledge, attitudes, and preventive behaviours.

2.7. Administration of the Instrument

The WhatsApp Cybercrime Awareness and Prevention Questionnaire (WCAPQ) was administered to the selected sample of 400 undergraduate students across higher institutions in Ekiti State, Nigeria. Permission was first obtained from the appropriate institutional authorities, and respondents were briefed on the purpose of the study, ensuring informed consent. The questionnaires were distributed by trained research assistants. The completed questionnaires were collected immediately or within a specified period to ensure a high response rate and data accuracy.

2.8. Data Analysis

The data collected from the WhatsApp Cybercrime Awareness and Prevention Questionnaire (WCAPQ) were organised, coded, and analysed using descriptive and inferential statistics. Descriptive statistics, such as frequencies, percentages, means, and standard deviations, were used to summarise students' responses regarding their use of WhatsApp and their knowledge, attitudes, and preventive behaviours related to cybercrime. Inferential statistics, including regression analysis was employed to test the hypotheses.

3. Results

3.1. Descriptive Analysis

Question 1: What is the level of awareness of cybercrime threats among students in higher institutions through the use of WhatsApp learning platform?

Students' awareness of cybercrime threats through the use of WhatsApp learning platform was generally moderate. As indicated in Table 1, specifically, 40% of respondents reported moderate awareness of phishing, while only 10% were very aware, resulting in a mean score of 3.20. Similarly, awareness of identity theft and hacking showed moderate levels, with mean scores of 3.10 and 3.20, respectively. Awareness of cyberbullying and online fraud was slightly higher, with mean scores of 3.50 and 3.40, yet still within the moderate range.

Table 1 Descriptive Analysis of responses on level of awareness of cybercrime threats among students.

Cybercrime Threat	Not Aware (1)	Slightly Aware (2)	Moderately Aware (3)	Aware (4)	Very Aware (5)	Mean Score	Remark
Phishing	20 (5%)	60 (15%)	160 (40%)	120 (30%)	40 (10%)	3.20	Moderate
Identity Theft	30 (7.5%)	70 (17.5%)	150 (37.5%)	120 (30%)	30 (7.5%)	3.10	Moderate
Cyberbullying	15 (3.8%)	50 (12.5%)	140 (35%)	130 (32.5%)	65 (16.2%)	3.50	Moderate
Hacking	25 (6.2%)	80 (20%)	150 (37.5%)	110 (27.5%)	35 (8.8%)	3.20	Moderate
Online Fraud	20 (5%)	70 (17.5%)	140 (35%)	120 (30%)	50 (12.5%)	3.40	Moderate

Question 2: How effective are WhatsApp learning platforms in enhancing students' knowledge of cybersecurity practices?

The WhatsApp learning platform was generally effective in enhancing students' knowledge of cybersecurity practices, as shown in Table 2. Many students agreed or strongly agreed that WhatsApp helped them identify phishing emails (mean = 3.8), improved their understanding of secure websites (mean = 3.7), encouraged the use of strong passwords (mean = 3.5), promoted safe online behaviour (mean = 3.6), and increased awareness of online fraud (mean = 3.6).

Table 2 Descriptive Analysis of responses on the effectiveness of WhatsApp learning platforms in enhancing students' knowledge of cybersecurity practices.

Knowledge Item	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)	Mean Score	Remark
Helps identify phishing emails	15 (3.8%)	25 (6.2%)	90 (22.5%)	180 (45%)	90 (22.5%)	3.8	Effective
Improves understanding of secure websites	20 (5%)	30 (7.5%)	100 (25%)	170 (42.5%)	80 (20%)	3.70	Effective
Encourages use of strong passwords	25 (6.2%)	35 (8.8%)	110 (27.5%)	150 (37.5%)	80 (20%)	3.50	Effective
Promotes safe online behaviour	15 (3.8%)	30 (7.5%)	100 (25%)	170 (42.5%)	85 (21.2%)	3.60	Effective
Increases awareness of online fraud	20 (5%)	25 (6.2%)	110 (27.5%)	160 (40%)	85 (21.2%)	3.60	Effective

Question 3: To what extent do WhatsApp learning platform influence students' attitudes and behaviors toward cybercrime prevention?

Table 3 indicates that the WhatsApp learning platform had a moderate to high influence on students' attitudes and behaviours toward cybercrime prevention. The analysis showed that students reported being encouraged to report suspicious messages (mean = 3.8) and to exercise caution when sharing personal information online (mean = 3.7). Other behaviours, such

as updating passwords regularly (mean = 3.5), motivating peers to follow safe online practices (mean = 3.6), and reducing risky online behaviour (mean = 3.6), were influenced to a moderate extent.

Table 3 Descriptive Analysis of responses the extent to which WhatsApp learning platform influence students' attitudes and behaviors toward cybercrime prevention.

Behavioural Item	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)	Mean Score	Remark
Encourages reporting suspicious messages	20 (5%)	30 (7.5%)	90 (22.5%)	160 (40%)	100 (25%)	3.80	Moderate-High
Promotes caution in sharing personal information	25 (6.2%)	40 (10%)	90 (22.5%)	150 (37.5%)	95 (23.8%)	3.70	Moderate-High
Encourages regular password updates	30 (7.5%)	50 (12.5%)	110 (27.5%)	130 (32.5%)	80 (20%)	3.50	Moderate
Motivates peers to follow safe online practices	25 (6.2%)	40 (10%)	100 (25%)	150 (37.5%)	85 (21.2%)	3.60	Moderate
Reduces risky online behaviour	20 (5%)	35 (8.8%)	105 (26.2%)	155 (38.8%)	85 (21.2%)	3.60	Moderate

Question 4: What challenges are associated with the use of WhatsApp learning platform for cybercrime prevention education in higher institutions?

The challenges associated with using WhatsApp for cybercrime prevention education in higher institutions. Students reported that poor internet connectivity (mean = 3.7) and distractions from non-academic content (mean = 3.6) were moderate-to-high challenges. Other issues, including limited participation from some students (mean = 3.4), information overload (mean = 3.5), and technical difficulties with the platform (mean = 3.5), were experienced to a moderate extent. Therefore, while WhatsApp is an effective tool for learning, these challenges may hinder full engagement and limit the platform's potential in promoting cybersecurity awareness, as highlighted in Table 4.

Table 4 Descriptive Analysis of the responses on the challenges that are associated with the use of WhatsApp learning platform for cybercrime prevention education in higher institutions.

Challenge Item	Not a Challenge (1)	Minor Challenge (2)	Moderate Challenge (3)	Significant Challenge (4)	Major Challenge (5)	Mean Score	Remark
Poor internet connectivity	20 (5%)	40 (10%)	90 (22.5%)	120 (30%)	130 (32.5%)	3.70	Moderate-High
Distractions from non-academic content	25 (6.2%)	35 (8.8%)	100 (25%)	120 (30%)	120 (30%)	3.60	Moderate-High
Limited participation from some students	30 (7.5%)	50 (12.5%)	120 (30%)	110 (27.5%)	90 (22.5%)	3.40	Moderate
Information overload	25 (6.2%)	45 (11.2%)	110 (27.5%)	120 (30%)	100 (25%)	3.50	Moderate
Technical difficulties with the platform	30 (7.5%)	40 (10%)	110 (27.5%)	120 (30%)	100 (25%)	3.50	Moderate

3.2. Testing of Hypotheses

Hypothesis 1: The challenges associated with the use of WhatsApp learning platform will not significantly predict the level of awareness of cybercrime threats among students in higher institutions.

Table 5 presents the regression analysis examining the relationship between challenges associated with the use of the WhatsApp learning platform and students' awareness of cybercrime threats. The model summary shows an R^2 value of 0.283, indicating that approximately 28.3% of the variance in students' awareness of cybercrime threats was explained by the challenges associated with WhatsApp usage. The coefficients table also shows a statistically significant relationship (B = 0.452, t = 11.23, $p < 0.05$). However, given the descriptive survey design of the study, these findings should be interpreted as predictive associations rather than causal effects, since potential confounding variables were not controlled for in the analysis. Therefore, while the results suggest that perceived challenges are associated with students' awareness levels, they do not necessarily imply that the challenges directly caused changes in awareness. The observed relationship may be influenced by other contextual or environmental factors not examined in this study.

Hypothesis 2: The challenges associated with the use of WhatsApp learning platform will not significantly predict the effectiveness of WhatsApp learning platform in enhancing students' knowledge of cybersecurity practices.

The regression analysis, as presented in Table 6, examines the relationship between challenges associated with using the WhatsApp learning platform and its effectiveness in enhancing students' knowledge of cybersecurity practices. The model summary shows an R^2 value of 0.237, indicating that approximately 23.7% of the variation in knowledge enhancement was explained by the challenges encountered. The coefficients table indicates a statistically significant relationship (B = 0.385, t =

9.93, $p < 0.05$), suggesting that as perceived challenges increased, WhatsApp's effectiveness in improving students' cybersecurity knowledge also increased. However, given the descriptive survey design, these results should be interpreted as predictive associations rather than causal effects, as potential confounding variables were not controlled. This implies that while encountering challenges may be associated with greater engagement and knowledge acquisition, the relationship does not necessarily indicate that the challenges directly caused improvements in cybersecurity knowledge. Other factors, such as students' prior knowledge, motivation, or institutional support, may also influence this observed association.

Table 5 Regression Analysis of the prediction of level of awareness of cybercrime threats by challenges associated with the use of WhatsApp learning platform.

Coefficients	B	Std. Error	Beta	t	Sig.
Constant	1.224	0.098		12.49	0.000
Challenges	0.452	0.040	0.532	11.23	0.000
Model Summary					
Model	R	R^2	Adjusted R^2	Std. Error of Estimate	Model
1	0.532	0.283	0.280	0.412	1

Table 6 Regression Analysis of the prediction of effectiveness of WhatsApp learning platform in enhancing students' knowledge of cybersecurity practice by challenges associated with the use of WhatsApp learning platform.

Coefficients	B	Std. Error	Beta	t	Sig.
Constant	1.112	0.105		10.59	0.000
Challenges	0.385	0.039	0.487	9.93	0.000
Model Summary					
Model	R	R^2	Adjusted R^2	Std. Error of Estimate	
1	0.487	0.237	0.234	0.428	

4. Discussion

The fact that students displayed a medium degree of knowledge about cybercrime risks that include phishing, identity theft, hacking, cyberbullying, and online fraud indicates that digital technologies exposure does not necessarily result in a full understanding of cybersecurity. Although the student population interacts with the online world quite often, they might be mostly aware of it due to personal experience or informal sources of information as opposed to formal cybersecurity training. This confirms the fact that according to Nwajioha (2025), students in the tertiary institutions in Nigeria tend to have very little or no knowledge on matters related to cybersecurity as well as lacking the practical skills to identify and minimize cyber threats. The average level of awareness consequently reveals that there is a distance between online engagement among students and their ability to use their understanding on cybersecurity in practical situations online. Nevertheless, the result contrasts with Elom (2025), who has indicated a rather high rate of cybersecurity awareness among students at the Nigerian public universities. This variability can indicate institutional diversity in terms of the degree of focus on digital literacy and access to cybersecurity training, and the level of integration of technology in the teaching and learning process. The middle level of awareness can also be attributed to informal structure of WhatsApp, which despite being easy to use and interactive, might lack depth, structure, and evaluation systems that are traditionally linked to formal cybersecurity training. This means that although WhatsApp can be an effective complementary learning tool, it cannot completely be used to displace the structured learning methods.

The results that WhatsApp was typically useful in increasing cybersecurity practices awareness among students outline the possibility of social media to facilitate informal and collaborative learning. The reason why WhatsApp can be so effective in this context is that it has interactive aspects, including group discussions, instant messaging, and sharing multimedia content, which promote peer learning and constant interaction with educational content. The result is in line with Lee et al. (2023), who stated that WhatsApp use enhanced academic achievement and team effectiveness in a Malaysian privatized university, implying that mobile messaging tools may facilitate knowledge sharing and collaborative learning among learners. Nonetheless, the success of WhatsApp as a learning tool must be viewed with discretion as its educational value depends mostly on the use of the service. Research like Yilmazsoy (2020) also shows that overuse of WhatsApp in non-academic interactions can cause distraction, low concentration, and poor time management among the learners. This is an indication that knowledge may be learnt through the use of WhatsApp; however, without regulations, the application can deter such learning. Hence, the identified beneficial effects of the present study can be associated with the organized sharing of the content related to cybersecurity and the intentional interaction among the learning groups. The implication is that educational effectiveness of WhatsApp can be determined by the relevance and clarity of content shared, the level of student engagement and the degree of instructor control of discussions and control of students in learning activities. A well-designed utilization of WhatsApp as a component of an instructional procedure will thus benefit students in terms of learning about good cybersecurity practices but will not pose the risk of distraction.

The fact that WhatsApp was found to have moderate to high impact on the attitudes and behaviors of students in relation to cybercrime prevention indicates that social media learning tools can be significant in influencing not just knowledge but behavioral dispositions to the notion of being a safe online user. The interactive and collaborative WhatsApp can enable students to discuss cybersecurity concerns and spread experiences and get prompt feedback, which may enhance their sense of cyber threats and prompt responsible internet usage. This underscores the claim by Chaka et al. (2020) that social messaging applications can create more engagement in learning especially where conventional learning resources are scarce by promoting a sense of community, shared learning and shared responsibility among students. Nevertheless, the number of contextual factors that can define the level of influence of WhatsApp on real behavioral change could be large. As an example, Enyama (2021) found out that, even though WhatsApp enhanced communication and access to learning during the COVID-19 pandemic, it was not effective in establishing long-term behavioral change due to issues related to digital literacy differences, unstable internet access, and student engagement. It means that although WhatsApp can facilitate the development of positive attitudes in relation to cybersecurity practices, it can have only a limited effect in case students do not have the technology or other resources to ensure regular use. As a result, interactive learning strategies, including guided discussions, real-life examples of cybercrime cases, and sharing knowledge among peers, might need to be specifically applied to enhance the impact of WhatsApp on cybersecurity attitudes and behaviour among students to strengthen practical knowledge and stimulate the use of responsible online behaviours.

The study identified poor internet connectivity and distractions from non-academic content as significant challenges associated with using WhatsApp for cybercrime prevention education. These challenges highlight structural and behavioral barriers that can limit the effectiveness of social media–based learning platforms. In many developing contexts, unstable network connectivity and high internet costs can interrupt learning interactions, reduce participation in online discussions, and limit students' ability to consistently access shared educational materials. This finding aligns with Elom (2025), who identified high internet costs and poor network quality as major constraints affecting the effective use of WhatsApp and Telegram for academic support in Nigerian public universities. Similarly, Yilmazsoy (2020) noted that the presence of non-academic conversations and social distractions on WhatsApp can reduce students' focus on learning activities, thereby weakening the platform's potential as an educational tool. However, the challenges associated with WhatsApp use do not necessarily eliminate its educational value. For instance, Rabotapi (2024) reported that WhatsApp played a critical role in facilitating student engagement and academic support during the COVID-19 lockdown, even though issues such as limited digital literacy and infrastructural constraints were present. This suggests that the effectiveness of WhatsApp as a learning platform often depends on how well institutions and instructors manage its use and support students in navigating technological barriers. In this context, the challenges observed in the present study may reflect broader infrastructural and digital literacy gaps rather than limitations inherent to the platform itself. Addressing these barriers may therefore require institutional interventions such as improving internet accessibility, providing training to enhance students' digital literacy skills, and establishing clear guidelines for academic use of WhatsApp groups. Promoting responsible digital citizenship among students could also help minimize distractions and ensure that the platform is used more effectively to support cybersecurity awareness and education.

The study revealed that challenges encountered in using WhatsApp were significantly associated with students' awareness of cybercrime threats. This suggests that the conditions under which digital platforms are used for learning can shape how effectively students are exposed to and engage with cybersecurity information. When students experience barriers such as unstable internet connectivity, technical difficulties, or frequent distractions from non-academic content, their ability to consistently participate in learning interactions may be affected. Consequently, their exposure to discussions and educational materials related to cybercrime prevention may also vary. This observation aligns with previous studies, including Rabotapi (2024) and Elom (2025), which reported that infrastructural and technological barriers can influence students' engagement with digital learning platforms and, in turn, affect knowledge acquisition. Similarly, Yilmazsoy (2020) emphasized that usability and accessibility issues within digital platforms can shape how effectively learners gain awareness of online safety practices. However, the presence of challenges does not necessarily eliminate the educational value of collaborative messaging platforms. Studies such as Chib et al. (2021) and Enyama (2021) suggest that student motivation, peer interaction, and collaborative learning through messaging platforms can help mitigate some of the negative effects of technological barriers. Through group discussions, shared resources, and peer support, students may still develop a reasonable level of awareness even when challenges exist. This perspective may explain why students in the present study demonstrated a moderate level of awareness despite the challenges encountered in using WhatsApp. The implication is that while digital learning platforms offer opportunities for enhancing cybersecurity awareness, their effectiveness depends largely on the surrounding learning environment and support systems. Therefore, higher institutions may need to address infrastructural and contextual barriers—such as improving internet accessibility, providing technical support, and establishing guidelines for academic use of WhatsApp—to enhance students' engagement and strengthen awareness of cybercrime threats.

The study also found that challenges faced when using WhatsApp were significantly associated with its effectiveness in improving students' cybersecurity knowledge. This relationship suggests that the learning environment surrounding digital platforms can shape not only access to information but also the depth of students' engagement with educational content. While challenges such as unstable internet connectivity, message overload, and distractions from non-academic conversations

may initially appear to hinder learning, they can also indirectly influence how students interact with the platform and the strategies they adopt to acquire knowledge. Al-Mahrooqi and Denman (2020) observed that although mobile messaging platforms encourage knowledge sharing and collaborative learning, technical limitations and communication disruptions can influence how learners process and retain information. In contexts where connectivity interruptions occur, students may need to revisit messages, review shared materials repeatedly, or rely more heavily on peer explanations, which can sometimes reinforce learning through repetition and collaborative clarification. Furthermore, the finding reflects the adaptive nature of digital learning communities. According to Govil (2025), students often respond to technological challenges in messaging platforms by intensifying peer-to-peer interactions, engaging in problem-solving discussions, and collaboratively interpreting shared content. Such interactions can strengthen cognitive engagement and support deeper understanding of complex topics such as cybersecurity practices. In this sense, challenges do not always function solely as barriers; they may also prompt students to become more active participants in the learning process. However, when these challenges persist without adequate support, they may begin to undermine the overall effectiveness of the learning platform. As highlighted by Rabotapi (2024), unresolved infrastructural and technological barriers can reduce students' participation levels and weaken the consistency of digital learning interventions. From a broader perspective, this finding underscores the importance of balancing technological accessibility with structured instructional support when integrating social media platforms into educational contexts. The effectiveness of WhatsApp for cybersecurity education therefore depends not only on the availability of the platform but also on how learning activities are organized and supported. Structured moderation, clear academic guidelines, and purposeful integration of cybersecurity discussions can help transform potential challenges into opportunities for deeper engagement and collaborative learning. Consequently, higher education institutions may need to adopt a more strategic approach to the use of WhatsApp by combining technological infrastructure improvements with pedagogical guidance that encourages focused participation and sustained interaction with cybersecurity learning materials.

5. Conclusions

From this study, it is clear that WhatsApp can be a useful tool for teaching students about cybercrime and promoting safer online behaviour. Students showed a moderate understanding of cybercrime threats, meaning there is some awareness but room for improvement. The platform helped improve their knowledge and influenced their attitudes, but problems like poor internet connection, distractions, limited participation, and technical difficulties affected how much students could benefit. WhatsApp works well for cybercrime prevention education, but its effectiveness depends on addressing these challenges.

6. Recommendations

Based on the findings, it is recommended that universities need to enhance internet connectivity in order to facilitate a better online learning process to the students. There should also be clear guidelines that will limit the use of WhatsApp in education so as to minimize interruptions and maximize its efficiency. Moreover, the students are to be appropriately trained to use WhatsApp as a study tool, specifically to receive the knowledge on cybercrime prevention. WhatsApp groups are to be actively used when it comes to discussing, collaborate, and peer learning among the students. Moreover, sufficient technical assistance must be offered to respond to the challenges experienced when using the platform promptly. Lastly, the teaching of cybersecurity should be incorporated into the official curriculum, and WhatsApp can be used as a complement to support the learning process and encourage safe behaviors on the Internet.

Acknowledgment

The researcher acknowledges all students who participated in the study and the University authorities who permitted me to conduct the research with no barriers.

7. Declarations

7.1. Ethical considerations

To ensure confidentiality and privacy, students in this study were assured that their names and information would be kept confidential. The researcher informed the participants that they had the right to withdraw from the study at any time and were not coerced into sharing information if they felt uncomfortable doing so.

7.2. Use of artificial intelligence (AI)

The author declares that no generative artificial intelligence (AI) tools were used in the preparation, analysis, or writing of this manuscript.

7.3. Conflict of Interest

The author declares no conflicts of interest.

7.4. Funding

This research did not receive any financial support.

References

Abbasian, M. (2024). *Training through WhatsApp Messenger improves knowledge of health ambassadors on minor illnesses*. BMC Health Services Research. https://bmchealths ervre s.biomedcentral.com/articles/10.1186/s12913-024-11988-9

Al-Mahrooqi, R., & Denman, C. J. (2020). Using WhatsApp in higher education: Pedagogical benefits and challenges. *Education and Information Technologies, 25*(4), 3243–3260. https://doi.org/10.1007/s10639-019-10074-1

AP News. (2024, March 12). *Interpol's Operation Serengeti tackles rising cyber-enabled frauds across Africa*. https://apnews.com

Ayyoub, H. Y. (2022). Awareness of electronic crimes related to e-learning among students. *PMC*. Retrieved from https://pmc.ncbi.nlm.nih.gov/articles/PMC9568858/

Bandura, A. (1977). *Social learning theory*. Prentice Hall.

Bandura, A. (1986). *Social foundations of thought and action*. Prentice Hall.

Bhatnagar, N., & Pry, M. (2020). Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study. *Information Systems Education Journal*, 18(1). Retrieved from https://files.eric.ed.gov/fulltext/EJ1246231.pdf

Chaka, E., Smith, L., & Ncube, T. (2020). Enhancing open distance e-learning through social messaging applications. *Journal of Online Learning Research, 6*(3), 215–234.

Chib, A., Malik, S., & Laksmi, S. (2021). Peer-supported learning via mobile messaging applications: Implications for behavioral change in education. *Computers & Education, 168*, 104203. https://doi.org/10.1016/j.compedu.2021.104203

Cyberbullying Research Center. (2023). *Cyberbullying among university students: Trends, impacts, and responses*. https://cyberbullying.org

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*.

Elom, J. I. (2025). Digital tools in higher education: Opportunities and challenges in Nigeria. *Frontiers in Education,* 10, 1581514. https://www.frontiersin.org/articles/10.3389/feduc.202 5.1581514/full

Enyama, S. (2021). The effectiveness of WhatsApp for promoting online engagement during the COVID-19 pandemic. *International Journal of Educational Technology, 18*(1), 1–12. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8486629

E-Palli. (2022). *Student cybersecurity awareness survey report*. https://www.e-palli.org

eSentire. (2024). *Education sector ransomware trends report*. eSentire Cybersecurity Intelligence Reports.

Forbes. (2025, January 21). *Protecting our future: Why cybersecurity training is essential for students*. https://www.forbes.com/councils/forbestechcouncil/2025/01/21/protecting-our-future-why-cybersecurity-training-is-essential-for-students

Greeff, E. (2024). A case study of using WhatsApp as a scalable learning tool. *International Journal of Technology and Computer Science,* 14(2), 113–120. https://www.inderscien ceonline.com/doi/abs/10.1504/IJTCS.2024.139187

Higher Ed Dive. (2024, February 10). *Ransomware attacks on universities increase globally*. https://www.highereddive.com

IIETA. (2022). Cybersecurity awareness and phishing susceptibility among Nigerian engineering undergraduates. *International Journal of Safety and Security Engineering*, 15(3), 201–210.

Lee, C., Tan, K., & Lim, J. (2023). WhatsApp for collaborative learning in higher education: Impacts on knowledge retention and team effectiveness. *Education Sciences, 13*(3), 244. https://www.mdpi.com/2227-7102/13/3/244

Mansor, N. S. (2023). Data security knowledge on social media among students in Malaysian higher education. *ERIC*. Retrieved from https://files.eric.ed.gov/fulltext/ED639485.pdf

Mutair, A. A. (2025). WhatsApp-delivered education: Performance and satisfaction among undergraduate nursing students. *Journal of Nursing Education,* 64(1), 45–52. https://journals.h ealio.co m/doi/10.3928/01484834-20241120-04

Nwajioha, E. (2025). Cybersecurity awareness among students in Nigerian tertiary institutions. *Journal of Cybersecurity Education,* 12(1), 33–50. https://edufdns.ng/jcr eam/article/downlo ad/57/58

Rabotapi, A. (2024). Using WhatsApp to support learning during the COVID-19 lockdown: Challenges and opportunities. *Education and Information Technologies, 29*(5), 7585–7603. https://files.eric.ed.gov/fulltext/EJ1434262.pdf

Reuters. (2024, January 18). *Cybercrime damages to reach $9.5 trillion in 2024 – Report*. https://www.reuters.com

Schunk, D. H. (2012). *Learning theories: An educational perspective*. Pearson.

Sophos News. (2023, November 5). *Half of higher-education endpoints impacted by ransomware*. https://news.sophos.com

The Times. (2024, June 14). *University of the West of Scotland suffers massive data breach*. https://www.thetimes.co.uk

ThriveDX. (2024). *Project-based learning: Transforming cybersecurity education*. https://thrivedx.com/resources/article/project-based-learning-transforming-cybersecurity-education

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model. *Management Science*.

Yilmazsoy, A. (2020). Social media in higher education: Advantages, disadvantages, and impact on academic performance. *Journal of Education and Learning,* 9(4), 130–142. https://files.eric.ed.gov/fulltext/EJ1294075.pdf