INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)
ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

Cybersecurity Awareness of Students in AI-Assisted Learning Environments Using Adapted Human Aspects of Information Security Questionnaire (HAIS-Q)

Merch Jay P. Dollaga, Eduardo R. Yu II

Information Technology Department, General Santos City (Dadiangas), South Cotabato, Philippines

DOI: https://doi.org/10.51583/IJLTEMAS.2026.150700025

Received: 15 June 2026; Accepted: 20 July 2026; Published: 06 August 2026

ABSTRACT

The introduction of artificial intelligence (AI) in education has resulted in the transformation of teaching and learning practices but has also brought about new cybersecurity issues. The present study sought to assess the extent to which students have developed cybersecurity awareness skills in the context of AI-assisted learning and examine the relationship between AI-assisted learning experience and cybersecurity awareness. Quantitative descriptive-correlational research design involving 124 randomly selected participants was applied. Data were gathered through administration of the modified Human Aspects of Information Security Questionnaire (HAIS-Q) that proved to be highly valid (4.76) and reliable (Cronbach's Alpha = 0.967). The study employed descriptive statistics, Spearman Rank-Order Correlation, and Pearson Product-Moment Correlation to analyze the collected data. It emerged that participants had quite high cybersecurity awareness, measured by the overall average score of 4.16. The dimension of knowledge scored the highest (4.34), whereas behavior yielded the lowest mean (3.92). The correlation analyses revealed no statistically significant relationship between students' exposure to AI-assisted learning and cybersecurity awareness (Spearman $\rho = 0.058$, $p = 0.524$; Pearson $r = 0.001$, $p = 0.993$). The findings indicate that no statistically significant relationship was found between students' exposure to AI-assisted learning and cybersecurity awareness. Future studies should investigate additional variables, including digital literacy, AI literacy, cybersecurity education, institutional support, and prior cybersecurity experiences, to better explain variations in cybersecurity awareness. The findings highlight the need for educational institutions to strengthen cybersecurity awareness and AI literacy programs to promote responsible use of AI technologies.

Keywords: Cybersecurity Awareness, AI-assisted Learning, HAIS-Q, Information Security, Artificial Intelligence

INTRODUCTION

Cybersecurity awareness is increasingly important for students to develop an understanding of the concept of cybersecurity as the current generation of learners adopts AI-assisted learning technologies and other means of digital education. With the rise in the adoption of AI, intelligent tutoring, and other forms of technology within the educational sector, learners now face cybersecurity risks such as phishing, data theft, violation of privacy, and more. Research reveals that while the adoption of AI-assisted learning technologies increases educational opportunities and enhances learning experiences, it also exposes students to cybersecurity, privacy, and ethical risks that require responsible technology use and cybersecurity awareness.

Awareness of cybersecurity is usually gauged through the use of the Human Aspects of Information Security Questionnaire (HAIS-Q) (Parsons et al., 2017), and the measure looks at the Knowledge, Attitudes, and Practices (KAP) about information security for the participants being studied. Current literature shows that the HAIS-Q test is one of the most commonly utilized cybersecurity awareness measuring tools (Rohan et al., 2023). While various tests have been designed, previous research indicates that students tend to show only modest levels of cybersecurity awareness.

INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)
ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

Even as various forms of AI are gradually being incorporated into the process of learning in schools, there is inadequate scientific research on cybersecurity awareness in relation to the usage of AI-supported systems for learning purposes. The bulk of the research on cybersecurity awareness focuses on more traditional forms of e-learning and does not take into consideration any form of cybersecurity issues related to the use of AI technologies in education (McCormac et al., 2017).

This gap was filled by assessing the awareness of cybersecurity among students utilizing artificial intelligence-enabled learning tools via the Human Aspects of Information Security Questionnaire (HAIS-Q), which was used to capture the cybersecurity awareness of these students in regards to their Knowledge, Attitudes, Behaviors, and AI-enabled Security Practices. This study sought to establish whether there is any correlation between the use of artificial intelligence-enabled learning tools and cybersecurity awareness.

LITERATURE REVIEW

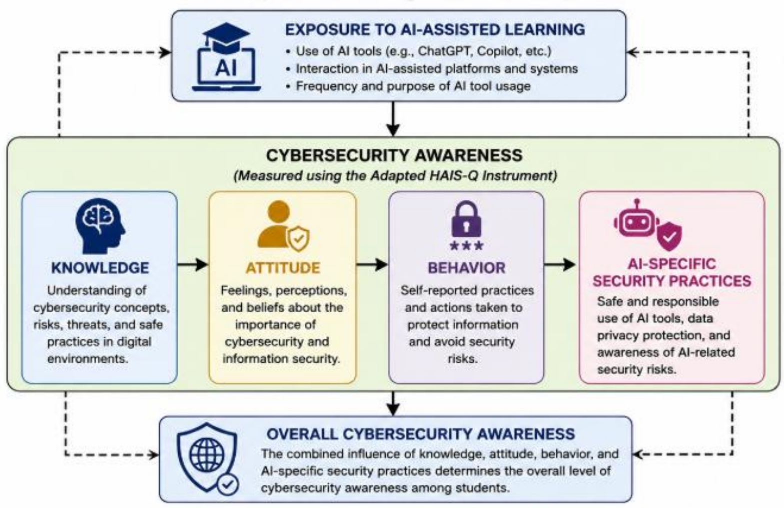
Theoretical Framework

The theoretical underpinning of this study is derived from the Knowledge-Attitude-Behavior (KAB) Model, which asserts that knowledge leads to attitudes, and attitudes lead to behavior. According to this model, individuals who have adequate knowledge of a particular area are likely to exhibit positive attitudes that lead to appropriate behaviors. In relation to cybersecurity, for example, it is assumed that individuals with adequate knowledge of cybersecurity threats, issues related to data privacy, and information security will be likely to have favorable attitudes towards cybersecurity and engage in appropriate behavior (Parsons et al., 2017; Zwilling et al., 2022). The questionnaire used in this study, namely, the Human Aspects of Information Security Questionnaire (HAIS-Q), is founded on the KAB model and assesses the respondents' cybersecurity awareness in terms of Knowledge, Attitude, and Behavior (Parsons et al., 2017). In this case, the KAB model has been expanded by including AI-Specific Security Practices in order to evaluate emerging issues in relation to cybersecurity and AI-assisted learning.

In this study, students' exposure to AI-assisted learning is treated as an external factor that may influence cybersecurity awareness through knowledge, attitudes, behaviors, and AI-specific security practices.

Figure 1

Theoretical framework of the study based on the Knowledge-Attitude-Behavior (KAB) Framework and the Human Aspects of Information Security Questionnaire (HAIS-Q).



The framework assumes that students' exposure to AI-assisted learning tools may influence their cybersecurity awareness through their knowledge of cybersecurity concepts, attitudes toward information security, online security behaviors, and AI-specific security practices. These dimensions collectively determine the overall level of cybersecurity awareness among students.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

Consequently, the study investigated the extent of cybersecurity awareness among students and established if there was a significant correlation between students' use of learning tools aided by artificial intelligence and their cybersecurity awareness.

Cybersecurity Awareness in Educational Environments

Cybersecurity awareness involves an individual's awareness of cybersecurity risks, safe internet usage practices, and their accountability when it comes to safeguarding their digital information. Cybersecurity awareness is very crucial in educational institutions since students interact with internet-based learning applications, cloud computing applications, and social media. With the increased use of technology in enhancing education within educational institutions, students have become susceptible to a wide range of cybercrimes, including phishing attacks, malware infection, identity fraud, and data breach (Setiawan & Rizal, 2021; Zwilling et al., 2022).

Various research studies have proven that cybersecurity awareness is an important factor in minimizing security threats caused by people. Students who have high cybersecurity awareness are able to perceive cyber threats and adopt safe internet use practices (McCormac et al., 2017; Zwilling et al., 2022). Students who possess high cybersecurity awareness have the ability to practice safe internet use practices, perceive the dangers around, and ensure sensitive data safety against any attacks (Setiawan & Rizal, 2021). Thus, cybersecurity awareness continues to be a major part of information security management.

Human Aspects of Information Security Questionnaire (HAIS-Q)

The Human Aspects of Information Security Questionnaire (HAIS-Q) is a widely used tool for measuring cybersecurity awareness. This questionnaire was developed by Parsons et al. (2017) and is based on three main aspects that include Knowledge, Attitude, and Behavior. According to the conceptual framework proposed by researchers, individuals that are knowledgeable about cybersecurity principles tend to have positive attitudes to information security, which eventually affects their behavior in terms of information security.

HAIS-Q is an extensively validated instrument with high levels of reliability when it comes to measuring information security awareness (Parsons et al., 2017). The systematic review of cybersecurity awareness instruments conducted by Rohan et al. (2023) showed that the Human Aspects of Information Security Questionnaire belongs to the group of the most frequently used and validated cybersecurity awareness tools. In view of the fact that the questionnaire is highly reliable and grounded in theory, it is widely used in various empirical studies, including research that involves students, employees, and other technology users. Additionally, findings of McCormac et al. (2017) confirmed that personal characteristics, including security attitudes, organizational cultures, and experience are among the factors influencing cybersecurity behaviors.

Cybersecurity Awareness Among Students

There are many studies focused on cybersecurity awareness among students. Specifically, previous studies have shown that although students often possess adequate cybersecurity knowledge, they do not always demonstrate secure online behaviors in practice (Hadlington, 2017; Perkasa & Setiawan, 2024). It shows that there is a huge gap between the knowledge about cybersecurity and cybersecurity practices itself.

In addition, Perkasa & Setiawan (2024) concluded that students exhibited good cybersecurity awareness in terms of password usage, information sharing, and protection of private information. These findings also suggest that educational programs for cyber behavior should target knowledge acquisition as well as proper cyber practices. Additionally, according to Hadlington (2017), students' cyber behavior is greatly determined by their impulsivity and addiction to the Internet. In this case, cyber awareness is often not enough to practice secure behaviors online.

Furthermore, the research conducted by Setiawan & Rizal (2021) showed that increased use of digital learning technologies led to improved awareness of cybersecurity issues. Moreover, Zwilling et al. (2022) suggested that cybersecurity knowledge, awareness, and behaviors can be considered interrelated factors contributing to enhanced cybersecurity practices. However, cyber awareness does not necessarily lead to safe cyber behavior.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

Institutions of learning contribute greatly to the process of raising cybersecurity awareness among learners. Prior research shows that cybersecurity education is extremely effective in improving learners' knowledge about online dangers, safety computing, and information security (Bada et al., 2019; Alharbi, T., & Tassaddiq, A, 2021). Such awareness campaigns typically deal with issues such as password safety, phishing, social engineering scams, privacy, and responsible Internet use. It is important for researchers to understand that cyber awareness is not just about knowledge but about behavioral changes as well. As Bada et al. (2019) point out, an awareness campaign works best when it helps users change their behavior and attitude towards cybersecurity rather than simply adding to their existing knowledge base. Regular training and repetition become essential since it is possible for an individual to know what to do but never actually put it into practice. That is why educational intervention remains critical for the promotion of cybersecurity awareness.

Artificial Intelligence in Education

The integration of generative artificial intelligence in higher education has led to increased possibilities for personalized learning, content creation, and academic assistance. Nevertheless, it has also brought forth the issue of academic integrity, as well as the need for digital literacy among students (Farrelly & Baker, 2023).

As AI-based tools like ChatGPT and their analogues become more popular, learners engage more with AI-assisted environments of instruction. With the development of AI-based instruction and integration of AI in the learning process, there is an increasing need for learners to demonstrate the skill set that would allow them to critically engage with AI-based technology (Ng et al., 2021; Biagini, 2025; Gu & Ericson, 2025).

Researchers have also pointed to the ethical aspects of using AI in education such as data privacy issues, bias within algorithms, and the need for transparency and accountability when using AI technology (Akgun & Greenhow, 2022; Pramod, 2025). However, the application of AI also comes with risks such as cybersecurity threats and privacy concerns as learners can unwittingly share confidential information or be exposed to risks associated with the security of AI environments.

Artificial Intelligence literacy refers to an individual's ability to understand, evaluate, and effectively use AI technologies while recognizing their limitations, ethical implications, and potential risks. Recent studies indicate that AI literacy has become an essential competency among students as AI-powered applications become increasingly integrated into educational environments (Ng et al., 2021; Gu & Ericson, 2025). Students who possess adequate AI literacy are better equipped to critically evaluate AI-generated information, identify misinformation, and use AI tools responsibly in academic activities (Ng et al., 2021; Hossain et al., 2025). According to Ng et al. (2021), AI literacy encompasses not only technical knowledge but also ethical awareness, critical thinking, and responsible decision-making. Recent studies further emphasize that AI literacy should include technical, ethical, social, and critical-thinking competencies to ensure the responsible use of AI technologies in educational settings (Kennedy & Gupta, 2025). As AI-assisted learning continues to expand, fostering AI literacy among students is becoming increasingly important for ensuring safe and effective technology use. AI literacy may also contribute to cybersecurity awareness because students who understand how AI systems function are more likely to recognize potential security and privacy risks associated with these technologies (Pramod, 2025).

Cybersecurity Risks in AI-Assisted Learning Environments

In recent times, increasing concerns regarding the cybersecurity threats posed by AI-powered learning tools have been observed in various studies. Recent studies indicate that the growing adoption of artificial intelligence technologies introduces new cybersecurity and privacy challenges that require continuous security awareness, risk management, and responsible technology use among learners (Xue, 2025; Chapagain et al., 2025). While this research was concerned with network security risks, the conclusion holds relevance here as well.

Learning environments assisted by AI technology might pose threats to students including data leakage, privacy breach, disinformation, prompt injection attacks, as well as unauthorized access to personal information. Current literature has pointed out the rising concerns in relation to privacy of AI, data governance, and handling of user information in learning environments at the university level (Xue, 2025; Chapagain et al., 2025). Given that AI

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

technologies constantly undergo fast development, conventional models of cybersecurity awareness might be insufficient in capturing the new security threats. In this respect, scholars have recommended modifying the existing cybersecurity awareness instruments based on the characteristics of the novel learning environment (Rohan et al., 2023). Campaigns and training programs play an essential role in promoting cybersecurity behaviors; however, their efficacy largely depends on their effect on users' attitudes and behaviors (Bada et al., 2019; Elkhodr & Gide, 2025).

METHODOLOGY

Research Design

Descriptive correlational research design was employed in this study. As stated by Creswell and Creswell (2018), the use of descriptive research involved describing the attributes, behavior, or condition of a population, while the correlational research involves finding the relationship between two or more variables without manipulation of these variables. The research design is applicable in measuring the level of variables and establishing the relationship between two or more variables without manipulation.

Specifically, the current study intended to describe the levels of cybersecurity awareness of students in AI-assisted learning environment as well as find out whether there exists a significant correlation between AI-assisted learning exposure and cyber security awareness among students. Descriptive analysis was performed to establish the level of cybersecurity awareness of students in terms of knowledge, attitude and behavior using the adapted HAIS-Q instrument. Correlational analysis was conducted to test for the correlation between variables under study.

Participants of the Study

The respondents of the study consisted of 124 students engaged in AI-assisted learning environments. Stratified random sampling was employed to ensure adequate representation of relevant subgroups based on academic program and year level. Population was stratified, and participants were chosen randomly from each stratum. According to Hair et al. (2019), a sample size exceeding 50 respondents is generally considered adequate for correlational studies. Therefore, the sample size of 124 respondents was deemed sufficient for the purposes of this study. Thus, the sample size in the present study could be regarded as adequate

Table 1

Socio-demographic characteristics (n=124)

Characteristics	Category	Frequency	Percentage
Gender	Male	95	76.61%
	Female	26	20.97%
	Prefer not to say	3	2.42%
BS Information Technology	1st Year	25	20.16%
	2nd Year	25	20.16%
	3rd Year	25	20.16%
	4th Year	25	20.16%
BS Computer Science	1st Year	6	4.84%
	2nd Year	6	4.84%
	3rd Year	6	4.84%
	4th Year	6	4.84%

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

Table 1 highlights the socio-demographic profile of the 124 respondents who participated in the study. With regards to gender, most respondents are males (95 respondents), while some are females (26 respondents), and few (3 respondents)of whom did not prefer to indicate their gender. This implies that the majority of respondents are male students.

In relation to the educational program pursued by the students, participants came from Bachelor of Science in Information Technology (BSIT) and Bachelor of Science in Computer Science (BSCS). In BSIT students, there were 25 respondents in first-year to fourth-year students. On the other hand, BSCS students were six respondents per year level, 124 participants in total.

This indicates that respondents from all year levels and both academic programs were represented in the sample.

Instrumentation and Data Gathering Process

The study involved the use of an adapted Human Aspects of Information Security Questionnaire (HAIS-Q) proposed by Parsons et al. (2017), which served as the main tool in collecting data for this study.

Students' experiences with AI-enabled learning were measured with a self-reported item measuring how often students had utilized the tools of AI assistance. Students rated their experience with AI-enabled learning technologies such as ChatGPT, Copilot, and others on a scale from “Never” through “Rarely,” “Sometimes,” “Often,” to “Always.”

Table 2

Adaptation matrix of the 16-item cybersecurity awareness questionnaire based on HAIS-Q and AI-specific security literature.

Item no.	Question	Dimension	Source/Adaptation Basis
1	I understand the importance of creating strong passwords.	**Knowledge**	Adapted from HAIS-Q Password Management domain (Parsons et al., 2017).
2	I am aware of phishing attacks and how they work.		Adapted from HAIS-Q Security Threat Awareness items.
3	I know the risks of sharing personal information online.		Adapted from HAIS-Q Internet Use and Information Handling items.
4	I understand how AI tools may store or use my data.		Developed from AI privacy and data governance literature (Xue, 2025).
5	I believe cybersecurity is important when using AI tools.	**Attitude**	Adapted from HAIS-Q Attitude dimension.
6	I feel responsible for protecting my personal data online.		

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

			Adapted from HAIS-Q Information Security Responsibility items.
7	I am concerned about privacy risks when using AI-assisted platforms.		Developed from AI privacy literature (Akgun & Greenhow, 2022).
8	I think following cybersecurity practices is necessary for students.		Adapted from HAIS-Q Attitude items.
9	I regularly update my passwords for online accounts.	**Behavior**	Adapted from HAIS-Q Password Behavior items.
10	I avoid clicking suspicious links or messages.		Adapted from HAIS-Q Email and Internet Use items.
11	I verify the security of websites before entering personal data.		Adapted from HAIS-Q Information Handling items.
12	I am careful about the information I input into AI tools.		Developed from AI security and privacy literature.
13	I avoid sharing sensitive information with AI tools.	**AI-Specific Security Practices**	Developed from AI privacy and security studies.
14	I review AI-generated responses before using them.		Developed from AI literacy literature (Ng et al., 2021).
15	I understand that AI tools may not always be secure or private.		Developed from AI cybersecurity literature.
16	I follow guidelines when using AI for academic purposes.		Developed from responsible AI use literature (Pramod, 2025).

Table 2 is a survey tool that was adapted according to the learning environment that involves artificial intelligence. This questionnaire consisted of four dimensions namely, Knowledge, Attitude, Behavior, and AI-related Security Practices. This adapted questionnaire consists of 16 Likert scale questions assessing students' knowledge regarding cybersecurity. Questionnaires have been widely used in quantitative research because they provide an organized and systematic approach in collecting data. A total of twelve items were amended from the initial Knowledge, Attitude, and Behavior factors, while four other items were created for addressing the cybersecurity issues related to AI-enabled learning environments. The AI-related items have been created based on relevant research related to AI literacy, data privacy, responsible AI usage, and cybersecurity.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

Table 3

Summary of Validators' Evaluation of the Questionnaire

Validator	Mean	Interpretation
Validator 1	4.86	Excellent
Validator 2	4.43	Very Good
Validator 3	5.00	Excellent
Overall Mean	4.76	Excellent

Table 3 shows the validators’ evaluations of the questionnaire. In validating the adapted instrument, experts in Information Technology and research gave the instrument a rating of 4.76 which is considered Excellent in terms of validity.

Table 4

Cronbach's Alpha Computation

Parameter	Value
Number of Respondents (n)	124
Number of Items (k)	16
Sum of Item Variances	15.18
Total Variance	163.00
Cronbach's Alpha	0.967
Interpretation	Excellent Reliability

`The modified HAIS-Q scale has a Cronbach's Alpha score of 0.967, which indicates excellent reliability with very strong internal consistency. This implies that all the questions in the scale are measuring the concept of cybersecurity awareness consistently. As suggested by Cronbach (1951), higher Cronbach's Alpha scores mean high internal consistency of survey questions. In addition, Parsons et al. (2017) identified that the HAIS-Q scale is a reliable scale for cybersecurity awareness measurement.

Data Analysis

Various descriptive and inferential statistical methods were used in analyzing the data collected in this study. The statistical tools used for data description included frequency, percentages, weighted mean, and standard deviation. These were applied in order to describe the levels of awareness of cybersecurity among the respondents regarding Knowledge, Attitude, Behavior, and AI-Specific Security Practices. Frequencies and percentages were used to show the demographic characteristics of the respondents and also the frequencies with which AI tools were used. Weighted mean helped to calculate the level of cybersecurity awareness in each of the four dimensions of cybersecurity. Standard deviation, on the other hand, helped to compute the variation in responses of the respondents.

To establish the existence of a significant relationship between students' use of AI-based educational technologies and cybersecurity awareness, Spearman Rank-Order Correlation served as the primary inferential statistical test because AI-assisted learning exposure was measured using an ordinal frequency scale ranging from Never to Always. To complement this analysis and examine the linear association between the variables, a Pearson Product-Moment Correlation was also performed as a supplementary analysis. The results were analyzed in terms of the calculated correlation coefficient value and direction, whereas the obtained p-value was used to test significance of the findings. The selected criterion for hypothesis testing included a significance

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

level of 0.05. If the p-value of the calculation was less than 0.05, the null hypothesis was rejected; otherwise, the study failed to reject the null hypothesis. Pearson's r is a widely used statistical measure for determining the strength and direction of the relationship between two quantitative variables.

To provide preliminary evidence of construct validity, Exploratory Factor Analysis (EFA) was conducted using Principal Component Analysis with Varimax rotation. Prior to factor extraction, the Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy and Bartlett's Test of Sphericity were performed to determine the suitability of the data for factor analysis. Eigenvalues, communalities, scree plot analysis, and rotated component matrices were examined in interpreting the factor structure of the adapted HAIS-Q instrument.

The study tested the null hypothesis stating that there is no significant relationship between students' exposure to AI-assisted learning and their cybersecurity awareness.

1. H_0: There is no significant relationship between students' exposure to AI-assisted learning and their cybersecurity awareness.

2. H_1: There is a significant relationship between students' exposure to AI-assisted learning and their cybersecurity awareness.

Research Ethics

This study was carried out in line with ethical standards applicable in human research studies. Before starting the study, the required approvals from the relevant parties were sought. Ethical concerns were kept in mind throughout the study so as to ensure the protection of the rights and well-being of the research participants. Human research should always be done in an ethical manner showing respect, beneficence, and justice to the people involved.

All research participants took part in the study on a voluntary basis. All the respondents were made aware of the purpose, aims, methodology, and importance of the study prior to being asked to participate in it. An informed consent form was distributed among all the research participants giving them information about their rights, one of which was their freedom not to participate in the study without suffering any repercussions.

Confidentiality and data security were guaranteed throughout the study process. In no way were any personal identifiers published in reports or presentations of the findings. The data provided remained anonymous and served research purposes only. The gathered data were stored safely and were available only to the researcher. All the information obtained was kept confidential and was presented in aggregate form.

Research Limitation

There are various limitations of the current study that need to be acknowledged. Firstly, only 124 participants were included in the study, all being students of one higher education institution. Secondly, the survey was conducted via a self-report questionnaire. In this regard, the findings were subject to response bias as well as social desirability bias because the responses provided by the students depended entirely on their honesty. Thirdly, the cross-sectional research design used in the study entailed the collection of data at one point in time. Consequently, it was impossible to identify the causal relationship between the variables, and only associations between them could be observed. Fourthly, the current study examined only the connection between AI-assisted learning and cybersecurity awareness but failed to take into account such factors as cybersecurity training, digital literacy, experience in cybersecurity matters, institutional resources, among others. Therefore, the findings should be interpreted with caution and may not be generalized to all higher education institutions.

Another limitation of the study is the measurement of AI-assisted learning exposure using a single self-reported frequency item. While this measure captured how often students used AI tools, it did not account for the duration of use, specific purposes, types of AI technologies utilized, or level of engagement. Future studies should employ more comprehensive measures of AI-assisted learning exposure to better capture the complexity of students' interactions with AI technologies.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

The study relied exclusively on quantitative survey data. Follow-up interviews or focus group discussions were not conducted and may have provided deeper insights into the reasons underlying the non-significant relationship between AI-assisted learning exposure and cybersecurity awareness. Future research may adopt mixed-methods approaches to obtain a more comprehensive understanding of students' experiences in AI-assisted learning environments.

FINDINGS AND DISCUSSION

Construct Validity of the Adapted Human Aspects of Information Security Questionnaire (HAIS-Q)

Table 5

KMO Measure and Bartlett's Test of Sphericity

Test	**Value**
KMO Measure of Sampling Adequacy	0.915
Bartlett's Test χ^2	2345.78
df	120
p-value	<.001

To provide additional evidence of construct validity, Exploratory Factor Analysis (EFA) was conducted on the 16-item adapted HAIS-Q instrument. Prior to factor extraction, the Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy and Bartlett's Test of Sphericity were performed. Results revealed excellent sampling adequacy (KMO = .915). Bartlett's Test of Sphericity was statistically significant, $\chi^2(120) = 2345.78$, $p < .001$, indicating that the correlation matrix was suitable for factor analysis. These findings support the appropriateness of conducting factor analysis for the adapted instrument.

Table 6

Total Variance Explained

Factor (Dimension)	**Eigenvalue**	**Percentage**
1	10.948	67.87%
2	1.225	7.60%
3	0.780	4.83%
4	0.754	4.67%

Although the sample consisted of 124 respondents, previous methodological studies have suggested that exploratory factor analysis may yield meaningful and stable results even with relatively small samples when sampling adequacy is high and the factor structure is well defined (MacCallum et al., 1999; de Winter et al., 2009). Given the excellent KMO value and significant Bartlett's Test, the use of EFA was considered appropriate for providing preliminary evidence of construct validity.

Exploratory factor analysis extracted two factors with eigenvalues greater than 1.00, accounting for 75.47% of the total variance. The first factor explained 67.87%, while the second factor explained 7.60% of the total variance.The remaining factors had eigenvalues below 1.00 and did not meet the Kaiser criterion for factor

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

retention. The results suggest that the adapted HAIS-Q items collectively measured a common underlying construct associated with cybersecurity awareness in AI-assisted learning environments.

Table 7

Communalities of the Adapted HAIS-Q Items

Item	Initial	Extraction
Item 1	1.000	**0.851**
Item 2	1.000	**0.667**
Item 3	1.000	**0.875**
Item 4	1.000	**0.723**
Item 5	1.000	**0.818**
Item 6	1.000	**0.833**
Item 7	1.000	**0.599**
Item 8	1.000	**0.870**
Item 9	1.000	**0.511**
Item 10	1.000	**0.772**
Item 11	1.000	**0.813**
Item 12	1.000	**0.769**
Item 13	1.000	**0.732**
Item 14	1.000	**0.705**
Item 15	1.000	**0.823**
Item 16	1.000	**0.814**

Table 7 presents the communalities of the adapted HAIS-Q items following principal component extraction. The extraction communalities ranged from 0.511 to 0.875, indicating that all questionnaire items were adequately represented by the retained components. Hair et al. (2019) recommend communalality values of 0.50 or higher as acceptable for interpretation. Since all 16 items exceeded this threshold, none of the questionnaire items required removal. These findings provide additional evidence supporting the construct validity of the adapted HAIS-Q instrument for measuring cybersecurity awareness in AI-assisted learning environments.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

Figure 2

Scree Plot of the Exploratory Factor Analysis for the Adapted Human Aspects of Information Security Questionnaire (HAIS-Q)

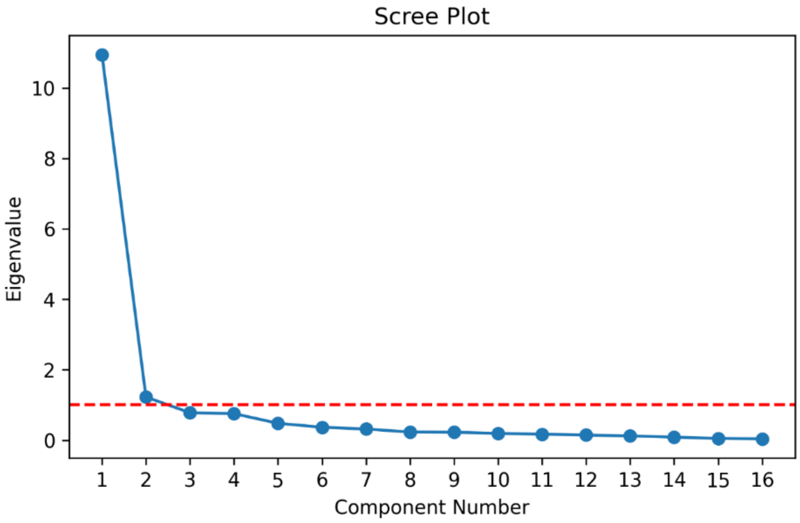


Figure 2 presents the scree plot generated from the exploratory factor analysis of the adapted Human Aspects of Information Security Questionnaire (HAIS-Q). The scree plot displays the eigenvalues of the extracted components in descending order and is used to determine the appropriate number of factors to retain. A pronounced decline in eigenvalues is observed between the first component (Eigenvalue = 10.948) and the second component (Eigenvalue = 1.225), followed by a gradual leveling off beginning with the third component. This point of inflection, commonly referred to as the "elbow," indicates that the first two components account for most of the meaningful variance in the dataset, while the remaining components contribute relatively little additional information.

Consistent with the Kaiser criterion, which recommends retaining components with eigenvalues greater than 1.00, two components were retained for further interpretation. The first component explained 67.87% of the total variance, whereas the second component explained an additional 7.60%, resulting in a cumulative explained variance of 75.47%. The scree plot therefore supports the retention of a two-factor solution, providing additional evidence for the construct validity of the adapted HAIS-Q.

Table 8

Rotated Component Matrix (Varimax Rotation)

Item	Component 1	Component 2
K1	**0.834**	0.393
K2	**0.673**	0.464
K3	**0.874**	0.333
K4	**0.754**	0.392
A1	**0.846**	0.320
A2	**0.836**	0.366
A3	**0.710**	0.307

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

A4	**0.860**	0.362
B1	0.059	**0.713**
B2	0.554	**0.682**
B3	0.446	**0.783**
B4	0.394	**0.784**
AI1	0.537	**0.666**
AI2	0.475	**0.692**
AI3	0.499	**0.757**
AI4	0.430	**0.793**

Table 8 presents the Varimax Rotated Component Matrix of the adapted HAIS-Q. Two interpretable components emerged following rotation. The first component consisted primarily of the Knowledge and Attitude items, with factor loadings ranging from 0.673 to 0.874, indicating that these items measure students' cybersecurity knowledge and attitudes toward secure technology use. The second component comprised the Behavior and AI-Specific Security Practices items, with factor loadings ranging from 0.666 to 0.793, reflecting students' cybersecurity behaviors and responsible AI-related security practices. Although several items exhibited moderate cross-loadings, each item demonstrated a stronger loading on one component, supporting the retention of all 16 questionnaire items. The rotated solution provides evidence that the adapted HAIS-Q measures two related but distinct dimensions of cybersecurity awareness among students in AI-assisted learning environments.

Table 9

Summary of the Extracted Factors from the Exploratory Factor Analysis of the Adapted Human Aspects of Information Security Questionnaire (HAIS-Q)

Factor	**Construct**	**Dominant Factor Loading Range**	**Interpretation**
Factor 1	Cybersecurity Knowledge and Attitudes	**0.673–0.874**	**Cybersecurity Knowledge and Attitudes.** This factor represents students' understanding of cybersecurity concepts, awareness of cyber threats, data privacy, and positive attitudes toward information security and the responsible use of AI-assisted learning technologies.
Factor 2	Cybersecurity Behaviors and AI-Specific Security Practices	**0.666–0.793**	**Cybersecurity Behaviors and AI-Specific Security Practices.** This factor reflects students' actual cybersecurity behaviors, including password management, safe online practices, protection of personal information, and responsible, secure use of artificial intelligence technologies.

Table 9 summarizes the interpretation of the two factors extracted through exploratory factor analysis. The first factor integrates the Knowledge and Attitude dimensions, indicating that students who possess greater cybersecurity knowledge also tend to demonstrate more positive attitudes toward information security. The second factor combines the Behavior and AI-Specific Security Practices dimensions, suggesting that secure online behaviors are closely associated with responsible use of AI technologies. Although the original HAIS-Q

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

conceptualizes cybersecurity awareness into four dimensions, the adapted instrument exhibited a two-factor structure within the present sample. This finding suggests that respondents perceived cybersecurity awareness as two broader but related constructs rather than four independent dimensions, thereby providing additional evidence of the construct validity of the adapted HAIS-Q.

Although the original Human Aspects of Information Security Questionnaire (HAIS-Q) was theoretically developed based on four dimensions—Knowledge, Attitude, Behavior, and Security Practices—the exploratory factor analysis conducted in this study extracted two broader factors. This finding suggests that respondents tended to perceive cybersecurity awareness in AI-assisted learning environments as two interrelated domains: cognitive awareness (knowledge and attitudes) and behavioral awareness (behavior and AI-specific security practices). Because exploratory factor analysis is sample-dependent, the observed two-factor structure should be interpreted as an empirical finding specific to the present sample rather than a replacement of the original theoretical framework. Future studies are encouraged to employ Confirmatory Factor Analysis (CFA) to validate the proposed factor structure.

Note: The extracted two-factor solution should be interpreted as an empirical representation of the responses obtained from the present sample rather than as a modification of the theoretical four-dimensional HAIS-Q framework.

Table 10

Level of Students' Cybersecurity Awareness by Dimension

Dimension	**Mean**	**Interpretation**
Knowledge	4.34	Very High
Attitude	4.24	Very High
Behavior	3.92	High
AI-Specific Security Practices	4.14	High
Overall	**4.16**	**High**

According to Table 10, students exhibit high levels of cybersecurity awareness in AI-enabled learning, with an average mean score of 4.16. Knowledge attained the highest mean score of 4.34, which was very high, meaning that students have adequate knowledge regarding cybersecurity. Attitude also received a very high rating with a score of 4.24, suggesting that respondents recognize the importance of cybersecurity and exhibit positive attitudes toward protecting personal and institutional information. Students have positive cybersecurity behavior had high means of 3.92. Their security practice within AI had high means of 4.14.

These results are in agreement with the research by Parsons et al. (Parsons et al., 2017; Zwilling et al., 2022; Chapagain et al., 2025), in which cybersecurity awareness was shown to be a result of cybersecurity knowledge, attitude, and behavior associated with the use of information systems. In addition, Setiawan & Rizal (Setiawan & Rizal, 2021) showed that cybersecurity awareness was increased among students was linked to consistent interaction with digital learning technology. Still, the relatively lower average result on the Behavior dimension implies that cybersecurity awareness does not necessarily ensure cybersecurity behavior. The finding corresponds to previous studies suggesting that cybersecurity knowledge does not necessarily translate into secure online behavior (Hadlington, 2017; Perkasa & Setiawan, 2024). On the one hand, a high Knowledge score means that students were aware of cybersecurity threats and the necessary safety measures. On the other hand, a relatively low Behavior score means that cybersecurity knowledge did not always guarantee consistent behavior. The reasons might be explained by convenience, habituation, or lack of cybersecurity skills. Hadlington (Hadlington, 2017) also observed similar results.

INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING,
MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)
ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

Figure 3

Distribution of Students According to AI Tool Usage Frequency.

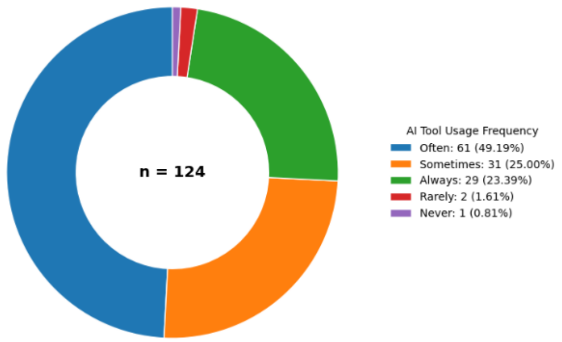


Figure 3 presents the frequency of AI tool usage among the 124 respondents. Most respondents reported using AI tools Often, with 61 students (49.19%). This was followed by 31 respondents (25.00%) who reported using AI tools Sometimes and 29 respondents (23.39%) who indicated Always. Only two respondents (1.61%) reported using AI tools Rarely, while one respondent (0.81%) indicated Never.

These findings show that AI-assisted learning tools are widely used among the respondents, with nearly three-fourths reporting that they use such tools often or always.The very high percentage of the respondents who stated that they frequently use AI learning tools implies the wide adoption of the technologies in question by students. It seems likely that one of the reasons is that such solutions allow obtaining and creating information, solving various problems, and gaining knowledge in the most efficient and convenient ways possible. Numerous studies prove that AI can be quite effective in engaging students and enhancing their education, so it is not surprising that they adopt AI solutions eagerly.

At the same time, frequent use of AI learning tools may imply that students get more and more comfortable with such software as part of the daily educational process. The regular use of AI might assist in improving productivity in terms of completing the assignments and accessing all needed resources easily. It is essential to state that, at the same time, such a high percentage implies certain responsibility for using AI, since numerous researchers claim that despite the obvious educational advantages, the risks associated with the misuse of AI technology cannot be ignored.

This conclusion reinforces recent studies showing that AI-enabled learning systems have become increasingly integrated into higher education and that AI literacy is becoming an essential competency for students in modern learning environments (Alblooshi, 2026).

Table 11

Spearman Rank-Order Correlation: Relationship Between Students' Exposure to AI-Assisted Learning and Cybersecurity Awareness

Variables	ρ	p-value	Decision	Interpretation
Exposure to AI-Assisted Learning and Cybersecurity Awareness	0.058	0.524	Fail to Reject H_0	Not Significant

Since AI-assisted learning exposure was measured using an ordinal frequency scale ranging from Never to Always, Spearman Rank-Order Correlation was employed to examine the relationship between AI-assisted learning exposure and cybersecurity awareness. The analysis revealed a weak positive correlation ($\rho = 0.058$)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

that was not statistically significant (p = 0.524). Therefore, the null hypothesis was not rejected. The findings indicate that the frequency of AI-assisted learning exposure was not significantly associated with students' cybersecurity awareness.

Table 12

Pearson Product-Moment Correlation: Relationship Between Students' Exposure to AI-Assisted Learning and Cybersecurity Awareness

Variables	r	p-value	Decision	Interpretation
Exposure to AI-Assisted Learning and Cybersecurity Awareness	0.001	0.993	Fail to Reject H_0	Not Significant

A supplementary **Pearson Product-Moment Correlation** was performed to compare the results obtained from the Spearman Rank-Order Correlation. The analysis revealed an **almost negligible positive correlation** between students' exposure to AI-assisted learning and cybersecurity awareness (**r = 0.001**), which was **not statistically significant** (**p = 0.993**). Consequently, the null hypothesis was **not rejected**, indicating that the frequency of AI-assisted learning exposure was **not significantly related** to students' cybersecurity awareness. The consistency of the Pearson and Spearman correlation analyses strengthens the conclusion that increased exposure to AI-assisted learning alone does not correspond to higher levels of cybersecurity awareness among the respondents.

Figure 4

Scatter Plot Showing the Relationship Between Students' Exposure to AI-Assisted Learning and Cybersecurity Awareness

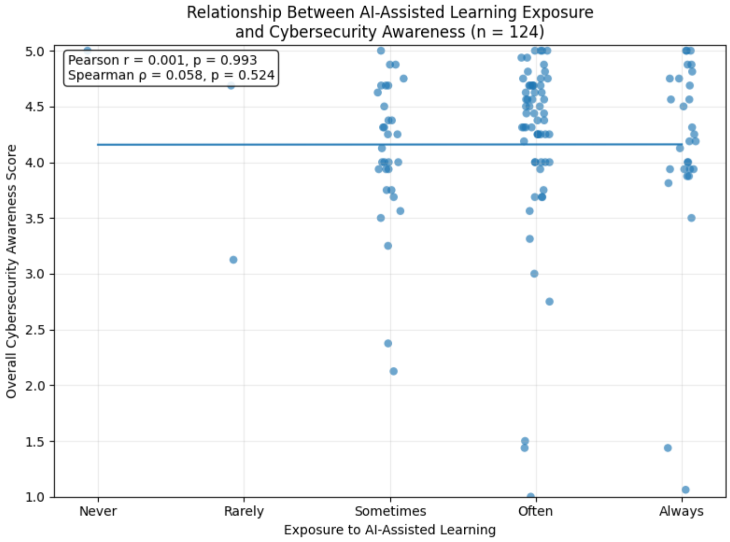


Figure 4 illustrates the relationship between students' exposure to AI-assisted learning and their overall cybersecurity awareness scores. Each point in the scatter plot represents one of the 124 respondents, with the horizontal axis indicating the frequency of AI-assisted learning exposure (Never, Rarely, Sometimes, Often, and Always) and the vertical axis representing the respondents' overall cybersecurity awareness scores based on the adapted Human Aspects of Information Security Questionnaire (HAIS-Q).

The scatter plot shows that respondents with both high and low cybersecurity awareness scores are distributed across all levels of AI-assisted learning exposure. There is no clear upward or downward pattern in the distribution of points, and the fitted trend line is nearly horizontal. This indicates that increasing exposure to AI-assisted learning does not correspond to a consistent increase or decrease in cybersecurity awareness.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

This visual pattern supports the statistical findings obtained from the correlation analyses. The Pearson Product-Moment Correlation indicated virtually no linear relationship between the variables ($r = 0.001$, $p = 0.993$), while the Spearman Rank-Order Correlation also showed a very weak and statistically non-significant monotonic relationship ($\rho = 0.058$, $p = 0.524$). Therefore, the frequency of AI-assisted learning exposure was not significantly associated with students' cybersecurity awareness in the present study.

Note: A small amount of horizontal jitter was applied to the plotted observations to improve the visibility of overlapping data points without altering their actual AI-assisted learning exposure values.

Based on the research results, it is possible to note that the use of AI tools does not affect the level of cybersecurity awareness among college students. While respondents actively applied artificial intelligence technologies during their studies, the use of such technologies may be oriented towards the efficient acquisition of new skills, increased productivity, and content creation but not the improvement of cybersecurity knowledge and practices. Consequently, students can develop skills in using AI tools while remaining unaware of cybersecurity issues.

At the same time, the presented results provide additional evidence of the complex nature of cybersecurity awareness. As explained by McCormac et al. (2017), individual and organizational factors influence the development of cybersecurity awareness and behavior. Furthermore, Rohan et al. (2023) argue that cybersecurity awareness is a multi-dimensional concept that requires continuous training.

The above finding also means that education establishments cannot rely on increased use of AI-related technological developments to enhance cybersecurity awareness among learners. There is need for deliberate cybersecurity awareness measures, literacy measures, and responsible AI usage education among others to make sure learners have the necessary knowledge, skills, and attitudes towards protecting themselves from cyber threats.

CONCLUSION

The study aimed to determine the cybersecurity awareness of students in AI-assisted learning environments using an adapted Human Aspects of Information Security Questionnaire (HAIS-Q). Based on the findings, it is noted that the respondents had a high level of awareness regarding their cybersecurity, as shown by the mean score of 4.16. In terms of the mean scores per dimension, it was observed that Knowledge obtained the highest mean score at 4.34. This means that students have great knowledge of cybersecurity, the threats involved when using the internet, and the dangers that might occur when using technology and AI learning methods.

The adapted measure proved to exhibit high psychometric properties. In terms of validity, the score was estimated at 4.76, while the value of Cronbach's Alpha was 0.967 in relation to reliability. Thus, one can conclude that the instrument under analysis was both reliable and valid, which made its use in order to assess cybersecurity awareness reasonable.

In addition, the study found no statistically significant relationship between students' exposure to AI-assisted learning and cybersecurity awareness, as indicated by both the Spearman Rank-Order Correlation ($\rho = 0.058$, $p = 0.524$) and the Pearson Product-Moment Correlation ($r = 0.001$, $p = 0.993$). As there is only a very weak positive correlation, which is not statistically significant, one may claim that frequent usage of AI does not make a significant contribution to cybersecurity awareness. Hence, the findings suggest that factors other than AI-assisted learning exposure may contribute to cybersecurity awareness among students. These factors may include cybersecurity education, digital literacy, institutional support, cybersecurity awareness campaigns, prior experiences with cyber threats, and information security training. However, these variables were not directly measured in the present study and therefore require further investigation.

The findings support the assumptions of the KAB Framework suggesting that knowledge, attitudes, and behavior interactions are necessary for the development of awareness and cannot be attributed solely to the experience of interacting with technology. As mentioned earlier, despite all advantages provided by the AI technologies in education, their proper and safe usage requires adequate cybersecurity skills and appropriate digital practices

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

among students. Thus, educational establishments must keep introducing cybersecurity courses and providing learners with chances to practice safe behaviors while using AI tools.

To sum up, the results show that today students who have access to the AI technologies have high levels of cybersecurity awareness. Nevertheless, the maintenance and further development of this awareness are vital since AI technologies will only become more popular and more advanced. In this regard, educational institutions should pay attention to developing cybersecurity awareness programs along with promoting AI literacy and relevant cybersecurity practices related to using AI technology.

The findings suggest that factors other than AI-assisted learning exposure may contribute to cybersecurity awareness. However, these factors were not directly examined in the present study.

Recommendation

From the results of this research, some recommendations can be made. First, educational organizations should raise cybersecurity awareness among students through seminars, workshops, and other training sessions dedicated to online security, data privacy, responsible use of digital technologies, and good cybersecurity practices. In addition, cybersecurity should be taught in class as part of the course, which will help students learn how to detect and address cybersecurity threats when using AI tools for educational purposes. Students are also advised to apply safe cybersecurity measures by choosing complex passwords, not clicking on suspicious links, protecting personal data, and confirming that the AI-generated content is authentic before incorporating it into their assignments. Also, future studies are encouraged to employ Confirmatory Factor Analysis (CFA) using larger and more diverse samples to validate the two-factor structure identified in the present study. Finally, the institutions are suggested to create a policy regarding the use of AI tools, which could contribute to minimizing the possible risks connected to their use in education. Replication of this research in other institutions with larger samples would be a useful step towards validating the results obtained. Future research could also investigate additional variables contributing to cybersecurity awareness, including cyber training, digital literacy, academic program, internet usage, and institutional factors, since the current study revealed that there was no association between the exposure to AI-assisted learning and cybersecurity awareness.

REFERENCES

1. Akgun, S., & Greenhow, C. (2022). Artificial intelligence in education: Addressing ethical challenges in K–12 settings. AI and Ethics, 2(3), 431–440. https://doi.org/10.1007/s43681-021-00096-7
2. AlBlooshi, S. (2026). Artificial intelligence in higher education: Opportunities and challenges: A review. Frontiers in Education, 10, Article 1683968. https://doi.org/10.3389/feduc.2025.1683968
3. Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. Big Data and Cognitive Computing, 5(2), 23. https://doi.org/10.3390/bdcc5020023
4. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv. https://doi.org/10.48550/arXiv.1901.02672
5. Biagini, G. (2025). Towards an AI-literate future: A systematic literature review exploring education, ethics, and applications. International Journal of Artificial Intelligence in Education, 35(4), 2616–2666. https://doi.org/10.1007/s40593-025-00466-w
6. Chapagain, D., Kshetri, N., & Pokharel, B. P. (2025). AISCliteracy: Assessing artificial intelligence and cybersecurity literacy levels and learning needs of students. arXiv. https://doi.org/10.48550/arXiv.2506.23321
7. Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. Psychometrika, 16(3), 297–334.
8. Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VII, July 2026

9. Elkhodr, M., & Gide, E. (2025). Integrating generative AI in cybersecurity education: Case study insights on pedagogical strategies, critical thinking, and responsible AI use. arXiv. https://doi.org/10.48550/arXiv.2502.15357
10. Farrelly, T., & Baker, N. (2023). Generative artificial intelligence: Implications and considerations for higher education practice. Education Sciences, 13(11), 1109. https://doi.org/10.3390/educsci13111109
11. Gu, X., & Ericson, B. J. (2025). AI literacy in K–12 and higher education in the wake of generative AI: An integrative review. arXiv. https://doi.org/10.48550/arXiv.2503.00079
12. Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346
13. Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). Multivariate data analysis (8th ed.). Cengage Learning.
14. Hossain, S., Khanam, S., Haniya, S., & Nasr, N. R. (2025). AI literacy and LLM engagement in higher education: A cross-national quantitative study. arXiv. https://doi.org/10.48550/arXiv.2507.03020
15. Kennedy, K. J., & Gupta, A. (2025). AI & data competencies: Scaffolding holistic AI literacy in higher education. Thresholds in Education, 48(2), 182–201.
16. McCormac, A., Zwaans, T., Parsons, K., Calic, D., Pattinson, M., & Butavicius, M. (2017). Individual differences and information security awareness. Computers in Human Behavior, 69, 151–156. https://doi.org/10.1016/j.chb.2016.11.065
17. Ng, D. T. K., Leung, J. K. L., Chu, S. K. W., & Qiao, M. S. (2021). AI literacy: Definition, teaching, evaluation and ethical issues. Proceedings of the Association for Information Science and Technology, 58(1), 504–509. https://doi.org/10.1002/pra2.487
18. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 69, 105–118. https://doi.org/10.1016/j.cose.2017.01.004
19. Perkasa, D. A., & Setiawan, B. (2024). Measuring information security awareness level of high school students. MALCOM: Indonesian Journal of Machine Learning and Computer Science, 4(4), 1301–1308. https://doi.org/10.57152/malcom.v4i4.1461
20. Pramod, D. (2025). Decoding responsible AI use: The influence of digital literacy and ethical awareness. Cogent Education, 12(1), Article 2592371. https://doi.org/10.1080/2331186X.2025.2592371
21. Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. Heliyon, 9(3), e14234. https://doi.org/10.1016/j.heliyon.2023.e14234
22. Setiawan, B., & Rizal, M. A. (2021). Measurement of information security and privacy awareness in college students after the COVID-19 pandemic. https://doi.org/10.1016/j.procs.2024.03.138
23. Tian, J. (2025). Integrating artificial intelligence into the cybersecurity curriculum in higher education. Education Sciences, 15(11), 1540. https://doi.org/10.3390/educsci15111540
24. Xue, Y. (2025). A comparative analysis of AI privacy concerns in higher education. Education Sciences, 15(6), 650. https://doi.org/10.3390/educsci15060650
25. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, N. H. (2022). Cyber security awareness, knowledge and behavior: A comparative study. https://doi.org/10.1080/08874417.2020.1712269