

Journal of Politics and International Studies

Vol. 12, No. 1, January–June 2026, pp.200–220

Artificial Intelligence as a Predictor of Cybersecurity Awareness Among University Students: A Quantitative Study

Dr. Zahid Yaseen 

Associate Professor, Department of Politics & International Relation,
Government College Women University, Sialkot, Punjab, Pakistan

Corresponding: zahid.yaseen@gcwus.edu.pk

Dr. Muhammad Muzaffar 

Assistant Professor, Department of Politics & International Relation,
Government College Women University, Sialkot, Punjab, Pakistan

Email: muzaffarrps@gmail.com

Nayab Asghar 

Research Scholars, Department of Politics and International Relations,
Government College Women University, Sialkot, Punjab, Pakistan

Email: nayabasghar71@gmail.com

Arooj Fatima 

Research Scholars, Department of Politics and International Relations,
Government College Women University, Sialkot, Punjab, Pakistan

Email: arj27112002@gmail.com

Abstract

Artificial Intelligence (AI) has become essential part of today digital environment and university students are regularly using these technologies in educational and daily life activities. The aim of this study is to examine the relationship between cybersecurity awareness and artificial intelligence literacy among university students of Pakistan. The quantitative approach is used in this Study and data were collected from university students of Pakistan. By using Cochran formula minimum sample size was 384 but total 400 valid responses were collected through questionnaire. Findings indicate students have high AI literacy rate but their cybersecurity awareness level is moderate. Students are aware about AI basic concepts and potential misuse but the level of awareness about the phishing, suspicious links and cybersecurity issues and practical knowledge of reporting is very low. Study recommend that AI and cybersecurity education, training, and practical awareness programs are adding into university curriculum to enhance students' digital safety and cybersecurity skills.

Key Words: Cybersecurity, AL Literacy, Cybercrimes, Digital Skills, Cyber Threats, Phishing Awareness.

1. Introduction

The rapid development of digital technology has changed the ways of communication, study, and getting information. Today artificial intelligence become important part of modern digital environment. Now a days AI based applications are using for education purposes, content creations, communication, information searching and also other parts of the daily life. Universities students are regularly using the AI tools for educational as well as other purposes. AI learning has positive as well as negative aspects, it gives valuable opportunities for learning and provides access to information. On the other hand, by using it many concerns arise like data protection, privacy, misinformation, phishing, identity theft and their cyber threats. For this cybersecurity awareness in students has become major part of digital world. Cybersecurity awareness is the knowledge and understanding about recognition of the online threats, to protect personal accounts, devices, personal information and digital activities, and it helps in taking appropriate steps.

The rapid spread of AI has added new dimension to cybersecurity challenges. AI can support cybersecurity like to detect suspicious activities, identify potentials threats and in analyzing the large amount of data. But this technology can be used for creating false information, fraudulent messages, fake content and convincing phishing or social engineering attacks. The availability of AI these generated materials made it easier and convenience to create content like these. university has particular exposure because their academic and social lives are dependent on online learning systems, social media, cloud services, mobile applications and digital communication platforms. so their ability to recognise suspicious content and understand the digital risk are important for their online safety.

This issue needs special attention in university context where students are expected to use digital and AI-based technologies in academic activities. Limited awareness can have increased vulnerability of students against phishing, misinformation, privacy breaches, identity theft and other cyber threats. at this time research on relationship between AI literacy and cyber security awareness is limited. This research gap provides strong basis for present study. the aim of this study is to examine Artificial Intelligence as the predictor of Cybersecurity Awareness among the University Students. The findings of the study can help in developing initiative stronger AI and cybersecurity education for educators and universities. It can also support students in making safer and more informed decisions in the digital environment

II. Literature Review

Long and Magerko (2020) states that AI literacy is a set of competencies that enables individuals to understand, use, evaluate and communicate about AI. Similarly, Carolus et al. (2023) emphasized that AI literacy provide the ability to critically evaluate AI systems and their outputs which is important because of AI applications can produce information that appears reliable but may contain errors, bias or misleading content. Karger et al. (2023) developed an AI literacy test for university students and highlighted the importance of assessing students' actual understanding of AI rather than measure only their familiarity with AI tools. Further validation of

AI literacy measures has also shown that the concept involves several related competencies rather than a single technical skill (Koch et al., 2024).

University students represent an important group for studying AI literacy because they are among the frequent users of digital and AI-based technologies. AI applications are increasingly used for academic research, writing, translation, information searching, and other learning activities. However, regular use of AI does not indicate a strong understanding of the technology. Karger et al. (2023) found that AI literacy can vary among university students that shows that exposure to AI and actual knowledge about AI are not necessarily the same.

Alqahtani (2022) states that cybersecurity awareness alludes to an individual's understanding of cybersecurity threats and knowledge of appropriate measures for protecting digital information, accounts, devices, and online activities including awareness of risks such as phishing, malware, password attacks, identity theft and unauthorized access. However, cybersecurity awareness does not always translate into secure behaviour as users may recognize the existence of online threats but still engage in risky activities, such as using weak passwords, sharing personal information, or responding to suspicious messages. Hadlington et al. (2022) found differences in cybersecurity awareness and behaviour across educational groups and concluded that knowledge and actual behaviour should not be treated as identical concepts.

Cybersecurity practices refer to the actual actions individuals take to protect themselves and their information in digital environments which may include using strong and unique passwords, enabling additional security measures, updating software, checking website authenticity, avoiding suspicious links, and protecting personal information. Unlike cybersecurity awareness, which focuses on knowledge and understanding, cybersecurity practices are concerned with how that knowledge is reflected in everyday digital behaviour. Bognár and Bottyán (2024) emphasized the importance of measuring personal cybersecurity awareness and behaviour among university students through a structured assessment of security-related practices. The distinction between awareness and practice is important because individuals do not always behave according to what they know as a student may understand that phishing is dangerous but may still click on a suspicious link when the message appears convincing. Research on university students has therefore increasingly examined both awareness and behaviour rather than assuming that higher knowledge automatically leads to safer practices (Alqahtani, 2022; Bognár & Bottyán, 2024).

The development of AI has changed the cybersecurity environment in both positive and negative ways. AI can support cybersecurity by identifying unusual patterns, detecting threats, and processing large amounts of security-related information. At the same time, AI can also be used to improve the quality and scale of cyberattacks. The European Union Agency for Cybersecurity (ENISA, 2025) identifies the increasing use of AI as an important development in the contemporary cyber threat landscape. This makes it necessary for digital users to understand the changing nature of online threats.

Generative AI has also created new challenges for ordinary users because deceptive messages and digital content can become more convincing. Students may encounter AI-assisted phishing attempts, manipulated content, or other forms of digital

deception without knowing how such material was produced. A systematic review of cybersecurity among university students indicates that students remain an important population for cybersecurity research because their extensive digital engagement can expose them to a range of online risks (Nilupú-Moreno et al., 2024).

The relationship between AI literacy and cybersecurity awareness is gaining importance as AI becomes more integrated into digital environments. Butt, Malik, and Mahmood (2026), in a cross-sectional survey of Pakistani university students, reported a moderate overall level of AI literacy with no meaningful differences by gender or degree Programme, while Rashid, Malik, Abbas, and Khan (2024) found that most students viewed AI in a positive manner as a writing aid but had only a limited grasp of the AI tools actually generate their output. A comparable pattern outside the education sector appears in a national survey of healthcare students and professionals in Pakistan, which found strong self-reported familiarity with AI alongside inconsistent information and knowledge of its limitations (Habib, Hoodbhoy, & Siddiqui, 2024).

the literature reviewed here that revealed two reasonably and well-developed but largely separate strands of research: one concerned with defining and measuring AI literacy (Long & Magerko, 2020; Karger et al., 2023; Carolus et al., 2023; Koch et al., 2024), and another concerned with cybersecurity awareness and behaviour among university populations (Alqahtani, 2022; Hadlington et al., 2022; Bognár & Bottyán, 2024; Khan et al., 2023). Few studies bring these two strands together within a single framework, and fewer still do so in a Pakistani setting, where AI adoption among students is accelerating (Butt et al., 2026; Rashid et al., 2024) at a pace that appears to be outrunning the available evidence on students' cybersecurity preparedness. This leaves a clear empirical gap: it is not yet known, on the basis of Pakistani data, whether students who are more AI-literate are also more aware of cybersecurity risks or more likely to practice safe digital behaviour, or whether AI competence and cybersecurity competence develop largely independently of one another. The present study addresses this gap by examining AI literacy as a predictor of both cybersecurity awareness and cybersecurity practices among university students in Pakistan, treating the three constructs as conceptually distinct but empirically related, and thereby connecting an emerging area of research with a more established one.

III. Theoretical Framework

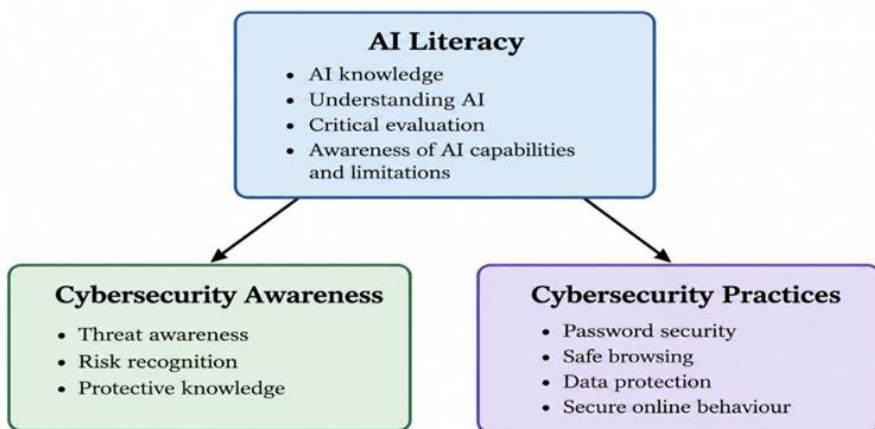
This study is based on the AI Literacy Competency Framework that proposed by Long and Magerko (2020). This framework defined that AI literacy as the ability to understand, use, evaluate, and critically engage with AI systems. It includes competencies related to the understanding of the AI capabilities and limitations, evaluation of AI-generated information, and recognition of the social and ethical implications of AI. These competencies provide a suitable theoretical basis for the examination of students' interaction with AI-enabled digital environments.

In the context of cybersecurity, AI literacy may influence how students recognize and respond to emerging digital risks. Students with stronger AI literacy may be better able to evaluate AI-generated content, recognize potential misuse of AI and understand privacy and security risks associated with AI-based technologies (Long

& Magerko, 2020; Carolus et al., 2023). However, AI literacy does not necessarily guarantee secure behaviour. Therefore, this study examines its empirical relationship with cybersecurity awareness and cybersecurity practices as separate outcomes.

Accordingly, AI literacy is treated as the predictor variable, while cybersecurity awareness and cybersecurity practices are treated as dependent variables. The framework provides a theoretical basis for testing whether differences in students' AI literacy are associated with differences in their awareness of cybersecurity risks and their reported security practices.

Fig 1: Conceptual Framework



IV. Material and Methods

Research Design

This basic study is descriptive and explanatory in nature, and employs a quantitative research approach to examine the relationship between AI literacy and cybersecurity awareness among university students in Pakistan.

Target Population and Sampling Technique

The target population of this study consists of university students enrolled in the undergraduate and postgraduate programs within the universities of the Sialkot district. **The simple random sampling technique** was used to reach the target population of this study.

The minimum sample size required for conducting this study is 384 respondents, determined by **Cochran's formula** at a 95% confidence level. However, in order to account for incomplete or unusable responses, a total of **400 valid responses** were collected for the study. The survey was conducted among university students through both online and offline modes.

Instrument of the Study

A structured questionnaire, comprised of four sections, was developed to collect primary data from the respondents. The first section consisted of demographic information while the second and the third section is consisted of 20 close-ended

statements. Both sections used a five-point Likert scale to measure the responses of participants. The response categories were **Strongly Agree (5), Agree (4), Neutral (3), Disagree (2), and Strongly Disagree (1)**. The fourth section consisted of **one open-ended question**, which allowed respondents to express their views about AI literacy and cybersecurity awareness.

Reliability and Validity

The validity of the research instrument was established through **content and face validity**. Expert review was used to identify ambiguous, irrelevant, or unclear statements before the final administration of the questionnaire. **Cronbach's Alpha was used in order to assess reliability of the instruments**. The reliability test was conducted to determine the internal consistency of the items used to measure the study variables. The reliability analysis was conducted using the Statistical Package for the Social Sciences (SPSS), and a Cronbach's Alpha coefficient of **0.70 or above** was considered an acceptable indication of internal consistency as shown in the table below:

Table 1: Reliability Analysis

	N	%
Valid Items	400	100.0
Excluded	0	.0
Total	400	100.0
Cronbach's Alpha	N of Items	
0.70	10	

Ethical Considerations

Ethical principles were followed throughout the research process. Participation in the study was voluntary, and respondents were informed about the purpose and nature of the research before completing the questionnaire. Participants were not required to provide information that could directly identify them, and the collected information was treated confidentially.

Respondents were given the option to decline participation or withdraw from the survey without any negative consequences. The collected data were used solely for academic and research purposes. The researcher also ensured that the responses were recorded and analyzed objectively without manipulation or alteration.

V. Results and Discussion

Table 2: AI Course and Cybersecurity Training

Response	Frequency	%
Yes	112	28
No	288	72
Total	400	100

Table 2 demonstrates that 72% people don't have any previous AI course and cybersecurity training, just 28% people have information and attend AI course and

cybersecurity training. This table shows that respondents' knowledge of AI and cybersecurity have been acquired through informal learning, personal experience, university education, or online sources rather than structured training.

Table 3: *Daily use of AI tools*

Field	Frequency	%
Less than 1 hour	128	32
1–2 hours	160	40
3–4 hours	64	16
More than 4 hours	48	12
Total	400	100

Table 3 demonstrates that 40% respondent used tools for 1-2 hour per day that shows he common usage category. About 32% people used AI for less than one hour and 16% Used for 3-4 hours and 12% used AI for more than 4 hours. Results indicate that use of AI tools were a regular part of respondents' daily activities.

Table 4: *Digital/Computer Proficiency*

Proficiency	Frequency	%
Beginner	32	8
Intermediate	256	64
Advanced	112	28
Expert	0	0
Total	400	100

Table 4 shows digital proficiency of the respondent, 8% respondent ranked themselves as beginner, 64% as intermediate and 28 % as advanced, the result identified that majority respondent have intermediate type of computer proficiency.

Artificial Intelligence Literacy

Table 5: *Basic concept about AI system*

Item no.	Statement	Level	F	%	Mean Score
1	Understanding about the basic concepts of how AI systems work (e.g., machine learning, algorithms).	SD	16	4	3.56
		D	16	4	
		N	144	36	
		A	176	44	
		SA	48	12	

Table 5 presents the level of understanding of respondents about the basic concepts of how AI systems work (e.g., machine learning, algorithms). 4% respondent strongly disagreed, 4% respondent disagreed, 36% remained neutral, 44% respondent agreed and 12% strongly agreed. The mean score indicate majority of people have understanding of fundamental concepts of AI.

Table 6: *AI and machine learning*

Item no.	Statement	Level	F	%	Mean Score
2	Understanding about roughly how AI, machine learning, and deep learning relate to one another.	SD	0	0	3.40
		D	64	16	
		N	144	36	
		A	10	40	
		AS	32	8	

Table 6 shows the level of understanding of how AI, machine learning, and deep learning relate to one another. 0% respondent strongly disagreed, 16% respondent disagreed, 36% remained neutral, 40% respondent agreed and 8% strongly agreed. The mean score 3.40 indicates moderate level of people have understanding AI, machine learning, and deep learning relate to one another.

Table 7: *Usage of AI tools*

Item no.	Statement	Level	F	%	Mean Score
3	Familiar with common AI tools and applications used today.	SD	0	0	3.76
		D	48	12	
		N	64	16	
		A	224	56	
		SA	64	16	

Table 7 presents the level of familiarity with common AI tools and applications used today. 0% respondent strongly disagreed, 12% respondent disagreed, 16% remained neutral, 56% respondent agreed and 16% strongly agreed. The mean score 3.76 indicates high level of level of familiarity with common AI tools and applications.

Table 8: *Learning and improvement*

Item no.	Statement	Level	F	%	Mean Score
4	AI systems learn/improve from the data they are given.	SD	32	8	3.68ss
		D	16	4	
		N	112	28	
		A	128	32	

SA	112	28
----	-----	----

Table 8 identifies the level of understanding that AI systems learn/improve from the data they are given. 0% respondent strongly disagreed, 12% respondent disagreed, 16% remained neutral, 56% respondent agreed and 16% strongly agreed. The mean score 3.68 indicates high level of understanding that AI systems learn/improve.

Table 9: Effective usage

Item no.	Statement	Level	F	%	Mean Score
5	Use of AI tools effectively for academic or personal tasks.	SD	16	4	4
		D	16	4	
		N	48	12	
		A	192	48	
		SA	128	32	

Table 9 identifies the level of ability to use AI systems in academic and other tasks. 4% respondent strongly disagreed, 4% respondent disagreed, 12% remained neutral, 48% respondent agreed and 32% strongly agreed. The mean score 4 indicates high level of ability to use AI systems effectively.

Table 10: Identification of tools

Item no.	Statement	Level	F	%	Mean Score
6	Can identify appropriate AI tools for a given task or problem.	SD	32	8	3.56
		D	48	12	
		N	64	16	
		A	176	44	
		SA	80	20	

Table 10 identifies the level of ability of respondent to identify appropriate AI tools for a given task or problem. 8% respondent strongly disagreed, 12% respondent disagreed, 16% remained neutral, 44% respondent agreed and 20% strongly agreed. The mean score 3.56 indicates high level of ability to identify appropriate AI tools effectively.

Table 11: Adoption of tools

Item no.	Statement	Level	F	%	Mean Score
		SD	16	4	

7	Feel confident in adapting to new AI tools and technologies.	D	96	24	3.36
		N	80	20	
		A	144	36	
		SA	64	16	

Table 11 identifies the level of ability of respondent to adapt new AI tools and technologies.4% respondent strongly disagreed, 24% respondent disagreed, 20% remained neutral, 36% respondent agreed and 26% strongly agreed. The mean score 3.36 indicates moderate level of adaptability towards new AI tools.

Table 12: Accuracy and reliability

Item no.	Statement	Level	F	%	Mean Score
8	Can critically assess the accuracy and reliability of AI-generated content.	SD	16	4	3.28
		D	80	20	
		N	128	32	
		A	128	32	
		SA	48	12	

Table 12 presents the ability of respondent to critically asses AI generated content.4% respondent strongly disagreed, 20% respondent disagreed, 32% remained neutral, 32% respondent agreed and 12% strongly agreed. The mean score 3.28 indicates moderate level of ability to critically assess AI generated content.

Table 13: Awareness

Item no.	Statement	Level	F	%	Mean Score
9	Aware about AI systems can produce biased or incorrect outputs.	SD	0	0	4.08
		D	0	0	
		N	80	20	
		A	208	52	
		SA	112	28	

Table 13 shows awareness of respondent that AI can produced biased or incorrect outputs. 0% respondent strongly disagreed, 0% respondent disagreed, 20% remained neutral, 52% respondent agreed and 28% strongly agreed. The mean score 4.08 indicates high level of awareness about possibility of biased or incorrect output.

Table 14: *Recognition of mistakes*

Item no.	Statement	Level	F	%	Mean Score
10	Can recognize that AI tools can make mistakes or give incomplete answers, even when they sound confident.	SD	16	4	4.04
		D	32	8	
		N	0	0	
		A	224	56	
		SA	128	32	

Table 14 presents the ability of respondent to recognize mistakes and incomplete answers generated by AI. 4% respondent strongly disagreed, 8% respondent disagreed, 0% remained neutral, 56% respondent agreed and 32% strongly agreed. The mean score 4.04 indicates level of ability high level to recognize mistakes and incomplete answers generated by AI.

Table 15: *Awareness about ethical issues*

Item no.	Statement	Level	F	%	Mean Score
11	Awareness of ethical issues related to AI use (e.g., privacy, data misuse).	SD	16	4	4.08
		D	0	0	
		N	32	8	
		A	240	60	
		SA	112	28	

Table 15 illustrates the awareness of respondent to ethical issues related to AI use (e.g., privacy, data misuse). 4% respondent strongly disagreed, 0% respondent disagreed, 8% remained neutral, 60% respondent agreed and 28% strongly agreed. The mean score 4.08 indicates level of awareness of ethical issues related to AI.

Table 16: *Potential risks*

Item no.	Statement	Level	F	%	Mean Score
12	Can understand the potential risks of sharing personal data with AI systems.	SD	32	8	3.84
		D	0	0	
		N	80	20	
		A	176	44	
		SA	112	28	

Table 16 illustrates the level of understanding s of respondent to potential risks of sharing personal data with AI systems. 8% respondent strongly disagreed, 0%

respondent disagreed, 20% remained neutral, 44% respondent agreed and 28% strongly agreed. The mean score 3.84 indicates high level of understanding regarding personal data risks.

Table 17: *Misuse of AI*

Item no.	Statement	Level	F	%	Mean Score
13	Awareness that AI can be misused for malicious purposes (e.g., deep fakes, phishing).	SD	0	0	4.04
		D	48	12	
		N	48	12	
		A	144	36	
		SA	160	40	

Table 17 presents the level of awareness of respondent Awareness that AI can be misused for malicious purposes (e.g., deep fakes, phishing).0% respondent strongly disagreed, 12% respondent disagreed, 12% remained neutral, 36% respondent agreed and 40% strongly agreed. The mean score 4.04 indicates high level of understanding regarding awareness.

Cybersecurity Awareness

Table 18: *Identification of common threats*

Item no.	Statement	Level	F	%	Mean Score
1	Can identify common types of cyber threats (e.g., phishing, malware, ransomware).	SD	16	8	3.12
		D	64	16	
		N	128	32	
		A	176	44	
		SA	0	0	

Table 18 presents the level of ability of respondent to identify common cybersecurity threats. 8% respondent strongly disagreed, 16% respondent disagreed, 32% remained neutral, 44% respondent agreed and 0% strongly agreed. The mean score 3.12 indicates moderate level of awareness regarding cyber threats.

Table 19: *Use of AI in Cybercrime*

Item no.	Statement	Level	F	%	Mean Score
2	Can understand how cybercriminals use AI to enhance attacks (e.g., AI-generated phishing emails).	SD	64	16	3.16
		D	48	12	
		N	80	20	
		A	176	44	
		SA	32	8	

Table 19 presents the level of understanding of how cybercriminals use AI to enhance attacks (e.g., AI-generated phishing emails). 16% respondent strongly disagreed, 12% respondent disagreed, 20% remained neutral, 44% respondent agreed and 8% strongly agreed. The mean score 3.16 indicates moderate level of understanding regarding use of AI by cybercriminal.

Table 20: *Risk of using public Network*

Item no.	Statement	Level	F	%	Mean Score
3	Awareness of the risks associated with using public Wi-Fi networks.	SD	48	12	3.36
		D	32	8	
		N	96	24	
		A	176	44	
		SA	48	12	

Table 20 presents the level of awareness of cybersecurity risks associated with the use of public Wi-Fi networks. 12% respondent strongly disagreed, 8% respondent disagreed, 24% remained neutral, 44% respondent agreed and 12% strongly agreed. The mean score 3.36 indicates moderate level of awareness of public waif risks.

Table 21: *Recognition of a suspicious email or website link*

Item no.	Statement	Level	F	%	Mean Score
4	Know how to recognize a suspicious email or website link.	SD	64	16	2.88
		D	80	20	
		N	112	28	
		A	128	32	
		SA	16	4	

Table 21 presents the level of ability to recognize a suspicious email or website link. 16% respondent strongly disagreed, 20% respondent disagreed, 28% remained

neutral, 32% respondent agreed and 4% strongly agreed. The mean score 2.88 indicates moderate level of ability to recognize suspicious emails and links.

Table 22: *Password for online accounts*

Item no.	Statement	Level	F	%	Mean Score
5	I use strong, unique passwords for different online accounts	SD	32	8	3.60
		D	32	8	
		N	96	24	
		A	144	36	
		SA	96	24	

Table 22 illustrates the level of practice of use of strong unique passwords for different online accounts. 8% respondent strongly disagreed, 8% respondent disagreed, 24% remained neutral, 36% respondent agreed and 24% strongly agreed. The mean score 3.60 indicates high level of awareness and practice regarding strong and unique passwords.

Table 23: *Login security*

Item no.	Statement	Level	F	%	Mean Score
6	Enable extra login security steps (e.g., two-factor authentication/2FA) where available.	SD	16	4	3.60
		D	64	16	
		N	96	24	
		A	2	28	
		SA	112	28	

Table 23 illustrates the level of understanding of two step authentication as a cybersecurity measure. 4% respondent strongly disagreed, 16% respondent disagreed, 24% remained neutral, 28% respondent agreed and 28% strongly agreed. The mean score 3.60 indicates high level of awareness regarding two-factor authentication.

Table 24: *Software update*

Item no.	Statement	Level	F	%	Mean Score
7	Regularly update my software and applications for security patches.	SD	16	4	3.00
		D	112	28	
		N	160	40	
		A	80	20	

SA	32	8
----	----	---

Table 24 illustrates the level of awareness of the important of software update security patches. 4% respondent strongly disagreed, 28% respondent disagreed, 40% remained neutral, 20% respondent agreed and 8% strongly agreed. The mean score 3.00 indicates moderate level of awareness regarding software update and security patches.

Table 25: *Clicking on unfamiliar links*

Item no.	Statement	Level	F	%	Mean Score
8	Avoid clicking on unfamiliar links or downloading unverified attachments.	SD	166	4	4.00
		D	16	4	
		N	80	20	
		A	128	32	
		SA	160	40	

Table 25 illustrates the level of tendency to avoid clicking on unfamiliar links or downloading unverified attachments. 4% respondent strongly disagreed, 4% respondent disagreed, 20% remained neutral, 32% respondent agreed and 40% strongly agreed. The mean score 4.00 indicates high level of awareness regarding safe online behaviour.

Table 26: *Cyber security*

Item no.	Statement	Level	F	%	Mean Score
9	Believe in cybersecurity is my personal responsibility, not just the institution's.	SD	32	8	3.48
		D	48	12	
		N	96	24	
		A	144	36	
		SA	80	20	

Table 26 shows the level of perception of personal responsibility for maintaining cybersecurity. 8% respondent strongly disagreed, 12% respondent disagreed, 24% remained neutral, 36% respondent agreed and 20% strongly agreed. The mean score 3.48 indicates high level of perceived personal responsibility for cyber security.

Table 27: Cybersecurity risks

Item no.	Statement	Level	F	%	Mean Score
10	Think carefully about cybersecurity risks before doing things online (e.g., downloading, clicking links, sharing information).	SD	16	4	3.72
		D	32	8	
		N	112	28	
		A	128	32	
		SA	112	28	

Table 27 shows the level of tendency of personal to think carefully about cybersecurity risks while using the internet. 4% respondent strongly disagreed, 8% respondent disagreed, 28% remained neutral, 32% respondent agreed and 28% strongly agreed. The mean score 3.72 indicates high level of awareness regarding online cybersecurity risks.

Table 28: Learning about protection

Item no.	Statement	Level	F	%	Mean Score
11	Motivated to learn more about protecting myself online.	SD	16	4	4.00
		D	32	8	
		N	48	12	
		A	144	36	
		SA	160	40	

Table 28 illustrates the level of motivation of personal to learn about protecting themselves online. 4% respondent strongly disagreed, 8% respondent disagreed, 12% remained neutral, 36% respondent agreed and 40% strongly agreed. The mean score 4.00 indicates high level of motivation to improve online protection.

Table 29: Review Privacy setting

Item no.	Statement	Level	F	%	Mean Score
12	Review privacy settings on social media and applications I use.	SD	0	0	3.56
		D	64	16	
		N	144	36	
		A	96	24	
		SA	96	24	

Table 29 presents the level of practice of reviewing privacy settings on social media and applications 0% respondent strongly disagreed, 16% respondent disagreed, 36% remained neutral, 24% respondent agreed and 24% strongly agreed. The mean score 3.56 indicates high level of awareness and practice regarding privacy setting.

Table 30: *Caution about personal information sharing*

Item no.	Statement	Level	F	%	Mean Score
13	Cautious about the personal information I share with AI tools and online platforms.	SD	16	4	3.40
		D	80	20	
		N	96	24	
		A	144	36	
		SA	64	16	

Table 30 presents the level of caution when sharing personal information with AI systems and online platform. 4% respondent strongly disagreed, 20% respondent disagreed, 24% remained neutral, 36% respondent agreed and 16% strongly agreed. The mean score 3.40 indicates moderate level of caution when sharing personal information with AI systems.

Table 31: *Subsection*

Item no.	Statement	Level	F	%	Mean Score
14	Know what steps to take if I suspect my account or device has been compromised.	SD	16	4	3.00
		D	144	36	
		N	112	28	
		A	80	20	
		SA	48	12	

Table 31 presents the knowledge of what to do if their account becomes compromised. 4% respondent strongly disagreed, 36% respondent disagreed, 28% remained neutral, 20% respondent agreed and 12% strongly agreed. The mean score 3.00 indicates moderate level of knowledge regarding appropriate responses to compromised accounts or devices.

Table 32: *Report center in university*

Item no.	Statement	Level	F	%	Mean Score
15		SD	48	12	2.64
		D	176	44	
		N	64	16	

Know where/who to report a cybersecurity incident to at my university.	A	96	24
	SA	64	4

Table 4.35 presents the knowledge Know where/who to report a cybersecurity incident to at my university.12% respondent strongly disagreed, 44% respondent disagreed, 16% remained neutral, 24% respondent agreed and 4% strongly agreed. The mean score 2.64 indicates moderate level of knowledge regarding reporting of cybersecurity incidents at the university.

Table 33: Mean Score Assessment

Statement No.	Mean score	Statement No.	Mean Score
1	3.56	1	4.04
2	3.40	2	3.12
3	3.76	3	3.16
4	3.68	4	3.36
5	4.0	5	2.88
6	3.56	6	3.60
7	3.36	7	3.00
8	3.28	8	4.00
9	4.08	9	3.48
10	4.04	10	3.72
11	4.08	11	4.00
12	3.84	12	3.56
13	4.04	13	3.40

Mean Average of 26 Statements =

Conclusion

Study concluded that university students have high artificial intelligence literacy but cybersecurity awareness level is moderate. Results concluded that students are more aware about common concept of AI tools, mistakes of AI generated content and possible misuse of AI. But the level of awareness about adaptation of new tools and critical evaluation power of students are relatively moderate. Cyber security means shows moderate level of familiarity among students to avoid unfamiliar link and attachment. Respondent have comparatively low awareness level to complain against issue at university. Results showed that AI literacy rate is much better but there is need of improvement in cybersecurity awareness and practical cybersecurity skills.

Recommendations

- Universities should organize AI and cybersecurity regular training and courses for all students.
- For understanding common cyber threats and safe online practices university should add cybersecurity in curriculum.
- Should organize practical training for student for to identify phishing emails, suspicious links and fake websites.
- University should spread awareness about what to do if their accounts are compromised
- There must have a clear cybersecurity incident reporting system in university for students.
- Should organize and arrange regular seminars, workshop and practical awareness campaign in university.

Conflict of Interest

The authors showed no conflict of interest.

Funding

The authors did not mention any funding for this research.

References

- Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences*, 12(5), 2589. <https://doi.org/10.3390/app12052589>
- Bognár, L., & Bottyán, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. *Education Sciences*, 14(6), 588. <https://doi.org/10.3390/educsci14060588>
- Butt, F. S., Malik, A., & Mahmood, K. (2026). Assessing AI literacy of university students in Pakistan: A cross-sectional survey. *Digital Library Perspectives*, 42(1), 141–158. <https://doi.org/10.1108/DLP-06-2025-0094>
- Carolus, A., Koch, M. J., Straka, S., Latoschik, M. E., & Wienrich, C. (2023). MAILS—Meta AI literacy scale: Development and testing of an AI literacy questionnaire based on well-founded competency models and psychological change- and meta-competencies. *Computers in Human Behavior: Artificial Humans*, 1(2), 100014. <https://doi.org/10.1016/j.chbah.2023.100014>
- Dawn. (2025, September 4). Governing AI [Editorial]. *DAWN.COM*. <https://www.dawn.com/news/1939562>
- European Union Agency for Cybersecurity. (2025). *ENISA threat landscape 2025*. European Union Agency for Cybersecurity.
- Habib, M. M., Hoodbhoy, Z., & Siddiqui, M. A. R. (2024). Knowledge, attitudes, and perceptions of healthcare students and professionals on the use of artificial intelligence in healthcare in Pakistan. *PLOS Digital Health*, 3(5), e0000443. <https://doi.org/10.1371/journal.pdig.0000443>
- Hadlington, L., Binder, J., & Gardner, S. (2022). The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates. *Education and Information Technologies*, 27, 11513–11532. <https://doi.org/10.1007/s10639-022-11077-8>
- Karger, E., Koren, G., & Wendt, S. (2023). What do university students know about artificial intelligence? Development and validation of an AI literacy test. *Computers and Education: Artificial Intelligence*, 5, 100165. <https://doi.org/10.1016/j.caeai.2023.100165>
- Khan, N. F., Ikram, N., Saleem, S., & Zafar, S. (2023). Cyber-security and risky behaviors in a developing country context: A Pakistani perspective. *Security Journal*, 36(2), 373–405. <https://doi.org/10.1057/s41284-022-00343-4>
- Koch, M. J., Carolus, A., Wienrich, C., & Latoschik, M. E. (2024). Meta AI literacy scale: Further validation and development of a short version. *Heliyon*, 10(21), e39686. <https://doi.org/10.1016/j.heliyon.2024.e39686>
- Long, D., & Magerko, B. (2020). What is AI literacy? Competencies and design considerations. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1–16). Association for Computing Machinery. <https://doi.org/10.1145/3313831.3376727>

Nilupú-Moreno, K., Salas-Riega, J. L., Ninaquispe-Soto, M., & Riega-Virú, Y. (2024). Cybersecurity in university students: A systematic review of the literature. In A. K. Nagar, D. S. Jat, D. K. Mishra, & A. Joshi (Eds.), *Intelligent sustainable systems* (pp. 315–332). Springer. https://doi.org/10.1007/978-981-99-7886-1_27

Pakistan Today. (2025, April 13). Cybersecurity and Pakistan. <https://www.pakistantoday.com.pk/2025/04/13/cybersecurity-and-pakistan/>

Rashid, S., Malik, S., Abbas, F., & Khan, J. (2024). Pakistani students' perceptions about knowledge, use and impact of artificial intelligence (AI) on academic writing: A case study. *Journal of Computers in Education*, 12, 1053–1078. <https://doi.org/10.1007/s40692-024-00338-7>

Schepman, A., & Rodway, P. (2023). The general attitudes towards artificial intelligence scale (GAAIS): Confirmatory validation and associations with personality, corporate AI use, and socio-demographic factors. *International Journal of Human-Computer Interaction*, 39(5), 1038–1052. <https://doi.org/10.1080/10447318.2022.2085400>

Tabash, M. I., et al. (2025). Cybersecurity knowledge, social networking, and awareness among Gen Z university students. *Discover Education*. <https://doi.org/10.1007/s44217-025-01084-3>

Zakar, R., Iqbal, S., Zakar, M. Z., & Fischer, F. (2021). COVID-19 and health information seeking behavior: Digital health literacy survey amongst university students in Pakistan. *International Journal of Environmental Research and Public Health*, 18(8), 4009. <https://doi.org/10.3390/ijerph18084009>