



Humaira Yasmeen¹ & Dr. Hafiz Kosar²

¹PhD Scholar Department of Education, National College of Business Administration & Economic Lahore, Multan (Alhamra University) Sub Campus, Punjab, Pakistan. E-mail: humairamalik36302@gmail.com

²Assistant Professor (HOD), Department of Education, National College of Business Administration & Economic Lahore, (Alhamra University) Multan Sub Campus, Punjab E-mail: drkousar.mul@ncbae.edu.pk

KEYWORDS	ABSTRACT
Cybersecurity awareness, University students, Social factors, Protective behaviours, Digital literacy, Cyber threats.	Although it is true that university students are more and more involved in digital technologies, they are also highly vulnerable to cyber security threats because of the lack of consistency in awareness and protective behaviours. This article is a combination of the latest empirical studies on the Cybersecurity awareness of Higher Education students, with a focus on social and technological components, and the latest systematic reviews on the subject. The surveys in Indonesia, Turkey, India, Bangladesh, Bahrain and the United States showed that students have the ability to report these same threats (phishing and malware), but those reports don't necessarily result in protection. Moreover, there are a number of reports that despite the fact that many students are aware about threats in cyber space, only a small number of them are formally trained in cyber security. The findings also suggest that perceived behavioural control is a factor affecting students' cybersecurity intentions, and that social learning is an important factor in shaping students' cybersecurity behaviour outside of the classroom. The article identifies the disconnect between the technical education in cybersecurity, which is mainly associated with the computing fields and the education in cybersecurity to all children/young people as an interdisciplinary field. The results indicate that structured cybersecurity training in the curriculum and the use of interesting pedagogical approaches like gamification and simulation can be implemented in universities.
ARTICLE HISTORY Date of Submission: 10-07-2026 Date of Acceptance: 13-08-2026 Date of Publication: 19-08-2026	 2026 Journal of Social Sciences Development
Corresponding Author	Humaira Yasmeen
Email:	humairamalik36302@gmail.com
DOI	https://doi.org/10.59075/jssd.v5i6.310
Volume/Issue	5(6), 2026, 157-166

Introduction

Today the digital technologies and e-learning platforms are revolutionizing the higher education sector, granting access, flexibility and convenience to students worldwide. This transformation to the cyber world has likewise brought new cyber security concerns, which can have a profound impact on the confidentiality, integrity and availability of education systems and personal information. In recent years, universities and students have declared that an escalating issue with sophisticated in scale with cyber threats remains a concern (Adeshola & Oluwajana, 2024; Duner et al., 2025).

There is an oxymoron in this digital world for the University student. Despite being an extremely tech-savvy group, they are still susceptible to phishing, malware, unauthorized access, and other online threats (Azad et al., 2025; Duner et al., 2025). Social media and mobile devices are also used regularly, which also increases the risk of encountering cyber incidents, particularly if people have no idea of the dangers of sharing personal information (Ahamed et al., 2026; Azad et al., 2025). That is, simply knowing how to be “digitally involved” won’t help create cyber security awareness and safe online behaviors.

Cybersecurity awareness research among university students often applies theoretical models such as Knowledge-Attitude-Behaviour (KAB) model, the Technology Acceptance Model (TAM) and the Theory of Planned Behaviour (TPB) or the Integrated Behavioural model (IBM) (Hasan et al., 2024; Rohan et al., 2025). The frameworks provide an understanding on how knowledge, attitudes, perceived behavioural control and intentions relate to cybersecurity practices. TPB framework has been used in different studies and some of them conclude that perceived behavioural control plays a more important role in determining intentions to practice cybersecurity; attitudes and subjective norms may be less significant in some cases (Saputra et al., 2026). In addition, cybersecurity behaviour research has found an important and strong antecedent of mindful awareness, with one study estimating that it accounted for 9.4% of the variance in cybersecurity behaviour among students (Yiit, 2025).

The education system is also weak in the area of cyber security. The authors of a systematic review also determined that 57.6% of cybersecurity education courses are limited to technical courses like computer science and engineering, excluding students in other courses (Mersni et al., 2025). I wish they'd have found a wider home as universities should not only have cybersecurity professionals they can churn out in sufficient numbers to meet demand but should have everyone their students can learn how to manage the digital threats. Hence, it is important to take an interdisciplinary approach to improve cybersecurity awareness, cybersecurity protection attitudes and behaviors, and to safe online interaction between disciplines (Rohan et al., (2025); Mersni et al., (2025)).

Objectives of the Study

1. To examine the level of cybersecurity awareness and preparedness among university students.

2. To investigate the social and technological factors influencing cybersecurity awareness and practices among university students.

Research Questions

1. What is the level of cybersecurity awareness and preparedness among university students?
2. Which social and technological factors influence cybersecurity awareness and practices among university students?

Methodology

The qualitative synthesis methodology followed by the researcher involves empirical studies in addition to the systematic review from the last couple of years (2020-2026). The synthesis combines the outcomes of multiple research designs used, which include quantitative surveys, qualitative interviews and mixed designs.

Data Sources and Selection

The review is directed by the papers obtained from the major academic databases (that is, Scopus, Web of Science, IEEE Xplore, ACM Digital Library and JSTOR). The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework, which was followed in similar systematic reviews, was used for selection. It selected the studies that included university/college students in cyber security awareness, knowledge, attitudes, and/or behaviours; peer-reviewed journals and conference proceedings; and English was the language of the studies.

Included Studies

The synthesis was based on results from a number of important empirical research studies and systematic reviews. The study by Hazari (2025) was a quantitative survey of 300 undergraduate students of The Assam Royal Global University (ARGU), Assam, India on the impact of cybersecurity breach on social media usage, awareness and protective behaviours of the participants. Students knew about cyber threats, but not completely prepared for the appropriate response via formal training or good practices.

The study involved 362 university students, analyzing the awareness and attitude, as well as students' cybersecurity decision making ability through intuitive or logical judgment, by applying the structural equation technique of partial least squares (PLS). To measure the cybersecurity awareness of the consumers it was used the concept of Theory of Planned Behaviour with a sample of 84 people, attitude, subjective norms, perceived behavioural control, intention, and behaviour were judged.

In accordance with this, a relational survey design with 179 undergraduate students was used by Yigit (2025) in a study to explain the relationship between mindful awareness and cybersecurity behaviours. The study results indicate a positive relationship between mindful awareness and

cybersecurity behaviour, which explained 9.4% of the variance in the students' cybersecurity behaviour.

In order to have a deeper understanding of the social learning environment and how it affects successful cybersecurity learning, Tokgoz and Xiang (2025) collected qualitative data in the form of interviews for 20 students and quantitative data for more than 150 students. They revealed that some learning environments such as informal settings and learning from peers had a significant role in developing cybersecurity knowledge concepts. Adama et al. (2026) conducted a survey of 236 computing students with an analysis of the nominal data obtained through thematic analysis and quantitative data. They found that students were generally aware, but persisted in having misconceptions and that they learned more about cybersecurity outside the classroom than through formal education.

Hasan et al. (2024) reviewed and analyzed 121 models and factors for the awareness of cybersecurity in e-learning, and Mersni et al. (2025) qualitatively reviewed and analyzed 125 peer-reviewed studies about interdisciplinary cybersecurity education. All these studies indicate that cybersecurity education is still limited to technical fields and it should be taught in a multidisciplinary approach.

Analytical Approach

In the synthesis, the data were analyzed through thematic analysis to identify patterns, themes and contradiction of the studies. Each element such as awareness levels, threat experiences, protective behaviours, social influences, educational factors and institutional structures were assigned a code that are then combined into themes that align with the purpose of the study. The results of the quantitative studies included were narratively synthesized and key statistics were reported if available.

Results

The synthesis reveals a pattern of students' basic knowledge of the common cyber threats and low level of preparedness in relation to such threats. Hazarika's study revealed that 72 percent of students were aware of certain threats, such as phishing, malware, identity theft and others, but only 25 percent said that they had received cyber security training. This same study showed that phishing was the most common type of attack and that many students suffering from it felt a loss of privacy, a disruption of their studies and felt anxious.

Social factors can impact on the awareness and behaviour of Cyber Security. The findings from the social learning environment study showed that learning about cybersecurity was occurring across social, YouTube, through friends/family, and formal. This reflects the fact that cybersecurity training and education is often informal and that individuals can acquire cybersecurity skills through their interactions and experiences in the world of electronic transactions.

The concept of mindful awareness was also seen as a good predictor of cybersecurity behaviour. It was moderately positively correlated with students' cybersecurity practices, and was a significant source of variance in Yigit's study. Similarly, a number of studies on the TBP theory suggest that in some situations perceived behavioural control outweighs attitude and subjective norms influences on intentions.

The results for the approaches to protect the technology are mixed. While many students use passwords, and privacy settings, a number of more sophisticated security options like two factor authentication and password managers are not used. This could result in students understanding the principles of security, but not use more effective security tools.

In cybersecurity education, many obstacles of structures have been observed in the literatures. A systematic review has found that so far, cyber security education still mainly focuses on training technical students, with little possibilities for interdisciplinary training of students from other fields of study. The review also highlighted the potential efficacy of the new and innovative technique of active learning that is more effective than the traditional classroom practice which includes project-based learning, gaming or simulation-based learning.

The synthesis demonstrates that generally speaking, student university population is aware of cyber dangers, but not necessarily exhibit protective behaviours. Students were aware of common threats such as phishing, malware and ID theft, and most have not had formal training on cyber security and don't use advanced tools and security features, such as two-factor authentication and password managers, regularly. According to the results, the disconnect between understanding of cyber risks and effective action to mitigate risks is still there.

It additionally exposes that social and psychological factor have a substantial impact on cybersecurity conduct. Students may learn about cybersecurity through informal sources (peers, family, social media and YouTube) not in formal classes. Moreover, perceived behavioural control and mindful awareness were also found to be significant factors in safer cybersecurity practices. The findings suggest that awareness levels, self-confidence and social learning all play a role in the attitude of the students to the online threats.

Based on the results, it can be concluded that the phenomenon of cybersecurity education is still constrained within technical fields and is lower in other courses in universities. The majority of the studies mentioned were lack of interdisciplinary access, less structured training and too much lecture method. There are some indications that alternative teaching approaches such as the use of active learning, experiential learning, project-based learning and simulation and gamification show greater potential but are not applied systematically. Conclusion from the synthesis: Broadly based and broaden education in cyber security for all students in universities is essential.

Discussion

This study, "Cybersecurity Awareness among University Students: A Social and Technological Study", further underscores the importance of robust digital security measures in educational

institutions. University students are one of the most digitally-engaging generations, adopting various online applications from smartphones up to laptops, social networks, learning management systems, electronic mail, cloud drives, and electronic banking across the board. But with this ubiquitous connection comes a myriad of vulnerabilities that warrant a deeper look. Interestingly, one of the observations that comes out of the research is that there is a considerable gap between the theoretical knowledge of the students on cyber risk and their practical decision making (Hossain, K. A. 2023)

Most participants showed an overall understanding of the typical risks of identity theft, malicious software, hacking and phishing scams, but do not necessarily practice this awareness in real-life situations. A student may even know the risks of following links that he has not received and opened, and even then he would be fooled by what looks like a trusted message sent from a contact who he knows either specially over WhatsApp or a social media platform such as email (Khalid, F. A. 2023).

There is major worry related to practices of password/key management. With so many different accounts that students have to access from institutional portals to personal email, social media accounts, cloud-based storage, and financial apps, there is a strong inclination for convenience over security. Many resort to having poor and insecure passwords or, worse yet, to reusing their passwords across multiple systems. This action is amplifying the possible impact of one account hack if there was a security problem the hacked account may give access to multiple other accounts (Peralta, A. (2024).

Also crucial is the social aspect of cyber security. Pupils are rooted in the digital social environment, using forums, messaging apps and communities. Such platforms, which can help with seamless communication and collaboration, can also become hotbeds for malicious activity. There are always challenges in the form of social engineering, fake profiles, misleading messages and violations of privacy. In many instances, through a lack of understanding of how information in many cases personally identifying information can be used against them, students unwittingly reveal themselves by posting their schedules, photos, school records, or other information that could be abused by malicious strangers (Citron, D. K. (2024).

The conversation indicates that there isn't any basic component to pupil cyber security awareness; as a substitute, a variety of factors come into play, such as technical competencies, social behaviors, individual threat perception, individual attitudes, and the level of institutional support. In the longer term, cyber security is cowed into the culture of university life could be beneficial, not just on an individual level. Intelligent and active students can help strengthen the anti-attack ability of the entire academic community, thereby enhancing the comprehensive security of educational institutions in the context of globalization (Hong & Xu 2023).

Conclusion

Based on the present review, there was a partial awareness of cybersecurity among the university students. Pupils have an understanding of typical threats online but are not always exhibiting appropriate behaviours to keep them safe, making it possible for them to become victim to cyberattacks and privacy breaches. Besides technical knowledge, social influences, self-efficacy, and informal learning experiences are also shown to be important for cybersecurity awareness.

The review further reveals that the current cyber security educating approaches are too subject based and too limited. As cybersecurity risks impact all students, it should be a shared responsibility for education and not be left to computer or engineering students alone. A more comprehensive and student-centered approach is needed to promote digital preparedness, awareness and engagement in a safer fashion within the Higher Education setting.

Recommendations

This may be expanded on in the future to investigate cyber security awareness in other academic disciplines, mainly non-technical, where there are few resources. Comparative studies between countries/universities/students also could provide insights into the effect of cultural and institutional aspects on cybersecurity behaviour. Longitudinal designs could be of great value in collecting evidence of whether behaviour has been sustained over time due to awareness/capacity building.

Furthermore, more studies are needed on the effectiveness of different educational methods, such as gamification, simulation-based learning, peer learning and cybersecurity education following the lines of mindfulness. Mixed methods investigations could also help to deepen in understanding students' attitude towards cyber threats and why sometimes awareness may not directly lead to action. More emphasis should also be placed on self-efficacy, perceived behavioural control and social learning in future studies as they appear to play a role in developing protective cyber security behaviors.

Practical Implications

There are implications for Higher Education Institutions.

The results have profound implications for the cybersecurity education of universities. First of all, such a structured cybersecurity education should be taken into account by institutions and keep open the integration of such learning into their curricula (not only in technical courses). With 25% of the student population not having formal cybersecurity training, there is a significant opportunity for improvement when it comes to affecting a wider range of students. Cyber security could be a common discipline taught in all universities as part of digital literacy studies of all students, irrespective of their academic qualification.

Second, the positive relationships exhibited between mindful awareness and cybersecurity behaviours indicate that educational interventions should adopt a mindfulness-based approach to promote students' mindful attention towards online security practices. Digital skills training programmes can effectively complement technology education and ensure reflective awareness of digital behaviors.

Third, the influence of perceived behavioral control on CBT turned out to be significant, suggesting that education efforts should also target students' confidence and self-efficacy to execute a cybersecurity action, not just threat awareness. The training that involves human touch and hands-on practise of security behaviours could be more effective than lecture-type teaching.

Pedagogical Recommendations

Based on evidence concerning pedagogical approaches, there are a few practical directions. Continued and enhanced use of active and experiential learning approaches – currently used in most successful programmes. The use of games and simulations identified as potentially effective from the literature was found to be of extra value for teaching students from non-technical backgrounds. There is a lack of collaborative and social learning, and a great opportunity to use informal learning from social media that students' peers and families are using to learn about cybersecurity. Considering the peer learning models, group projects, and awareness campaigns done with social media can be facilitated as educational interventions to improve learning. Inclusive pedagogical approaches to the teaching of learners are critical to access for learners from all disciplines. Using traditional techniques which involve jargon and lecture techniques create barriers for non-technical learners. Cybersecurity concepts can be communicated to a larger audience through the use of scenario-based learning, gamification and project-based approaches.

Policy and Institutional Recommendations

A Cyber Security failure of any kind seems to have repercussions on Institutional continuity and on the mental health of students made it necessary that Cyber Security is perceived as a matter of welfare of student and institutional responsibility. This involves clear policies on data protection, setting support systems for pupils who suffer from cyberattacks and involving cybersecurity awareness into orientation and continuous student development programmes. Institutional ambiguity – 16% of the studies examined in the samples were unclear about the target group and/or programme affiliation, indicating that universities should be more transparent about their programme structures and access to them.

Technological Implications

The lack of adoption of core security protections like the use of a two-factor or password managers could indicate that institutions need to make such tools more user-friendly, and actively promote them. Students might have to pass 2FA to log into their LMS and email accounts; this would make 2FA a standard process. Social Media privacy awareness is key as there is a

positive relationship between personal information sharing on social media and victimization. People should be reminded of the dangers of providing too much information online, especially in an educational setting, where students might not pay as much attention to privacy settings.

References

- Adama, V., Biddle, R., Arachchilage, N., & Lottridge, D. (2026). Confident yet concerned: Inconsistencies in computing students' attitudes on cybersecurity. *arXiv*.
- Adama, V., et al. (2026). Confident yet Concerned: Inconsistencies in Computing Students' Attitudes on Cybersecurity. *arXiv preprint arXiv:2606.18541*.
- Adeshola, I., & Oluwajana, D. I. (2024). Assessing cybersecurity awareness among university students: implications for educational interventions. *Journal of Computers in Education*. Springer.
- Ahamed, B., Polas, M. R. H., Falahat, M., Karim, R., & Tabash, M. I. (2026). Cybersecurity knowledge, social networking, and awareness among Gen Z university students. *Discover Education*, 5(1), 77.
- Alvito, G. B. N., Setiadi, F., & Irsan, M. (n.d.). Pengukuran Tingkat Kesadaran Keamanan Informasi Pada Mahasiswa Fakultas Informatika Menggunakan Human Aspect of Information Security Questionnaire (HAIS-Q) di Universitas Telkom Bandung. Universitas Telkom.
- Azad, R. U., Tasmim, S., & Atikuzzaman, M. (2025). Investigating students' awareness of online privacy and cybersecurity: an empirical study with effective cybersecurity training framework. *Global Knowledge, Memory and Communication*.
- Azad, R. U., Tasmim, S., & Atikuzzaman, M. (2025). Investigating students' awareness of online privacy and cybersecurity: An empirical study with effective cybersecurity training framework. *Global Knowledge, Memory and Communication*.
- Citron, D. K. (2024). The surveilled student. *Stan. L. Rev.*, 76, 1439.
- Dunder, I., Seljan, S., & Odak, M. (2025). Information Security Awareness in the University Environment: A Focus on Undergraduates. *TEM Journal*, 14(2), 1621-1628.
- Duner, I., Seljan, S., & Odak, M. (2025). Information security awareness in the university environment: A focus on undergraduates. *TEM Journal*, 14(2), 1621-1628.
- Hasan, M., et al. (2024). [Systematic review on models and factors influencing e-learning cybersecurity awareness].
- Hazarika, H. J. (2025). Impact of cybersecurity breaches on social media: A case study on undergraduate students.
- Hong, W. C. H., Chi, C., Liu, J., Zhang, Y., Lei, V. N. L., & Xu, X. (2023). The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. *Education and information technologies*, 28(1), 439-470.
- Hossain, K. A. (2023). Evaluation of technological breakthrough in global education and future employment opportunity. *Journal of Liberal Arts and Humanities (JLAH)*, 4(8), 1-62.

- Mersni, M., et al. (2025). [Systematic review on interdisciplinary cybersecurity education].
- Peralta, A. (2024). Best Practices for Managing Privacy and Security of Cloud-Based Student Data in Primary and Secondary Education.
- Rohan, R., Chutimaskul, W., Roy, R., Hautamäki, J., Funilkul, S., & Pal, D. (2025). Developing a scale for measuring the information security awareness of stakeholders in higher education institutions. *Education and Information Technologies*.
- Saputra, H. K., Giatman, M., Maksum, H., Lapisa, R., & Dwiyan, N. (2026). The Effects of Perceived Threat and Perceived Vulnerability on Security Awareness Through Cybersecurity Engagement. *Voteteknika (Vocational Teknik Elektronika dan Informatika)*, 14(1).
- Tokgoz, E., & Xiang, A. (2025). Social factors impacting cybersecurity students' learning and during decision making: The coverage of major-specific concepts.
- Yigit, M. F. (2025). Investigating the role of mindful awareness as an antecedent of university students' cyber security behaviors. *Journal of Learning and Teaching in Digital Age*, 10(2), 156–169.