TPM Vol. 32, No. S7, 2025
ISSN: 1972-6325
https://www.tpmap.org/



# AWARENESS OF CYBERSECURITY MEASURES AND STUDENTS' ACADEMIC PERFORMANCE

DR. UM E RUBAB
ASSISTANT PROFESSOR, DEPARTMENT OF EDUCATION, FATIMA JINNAH WOMEN UNIVERSITY RAWALPINDI, EMAIL: umerubab@fjwu.edu.pk

DR. HINA GUL
DEPARTMENT OF EDUCATION, FATIMA JINNAH WOMEN UNIVERSITY RAWALPINDI
EMAIL: hinagul469@gmail.com

DR. FARHA RAHMAN
DEPARTMENT OF EDUCATION, PIR MEHAR ALI SHAH, ARID AGRICULTURE UNIVERSITY RAWALPINDI,
EMAIL: farahrahman76@gmial.com

DR. SADIA ASLAM
DEPARTMENT OF EDUCATION, PIR MEHAR ALI SHAH, ARID AGRICULTURE UNIVERSITY RAWALPINDI,
EMAIL: sadiaaslam034@gmail.com

SHAD MUHAMMAD KHAN
DEPARTMENT OF EDUCATION, SHAHEED BENAZIR BHUTTO UNIVERSITY SHERINGAL DIR UPPER,
EMAIL: shadmuhammad44@gmail.com

MEHR BAKHT
DEPARTMENT OF EDUCATION, FATIMA JINNAH WOMEN UNIVERSITY RAWALPINDI
EMAIL: mehrbakht92@gmail.com

**ABSTRACT**
Cybersecurity awareness is a crucial competency that enables students to maintain safety and security in the online environment, safeguard their personal data, and cultivate responsible digital citizenship. There are various risks arising from the use of technology that impact students' motivation and cognitive abilities. In this regard, it is essential to make teachers aware of cybersecurity knowledge, as it can enhance students' psychological well-being, promote self-efficacy in digital learning, and improve their academic performance. The main purpose of the study is to find out the understanding of teachers regarding cybersecurity awareness and also check out the need and awareness of cybersecurity indicators for teachers and students. This research has the potential to offer significant insights into enhancing the design and execution of cybersecurity education initiatives, thereby fostering the safety, security, and responsible utilization of digital technologies. Descriptive research design was used in this study. Research survey was used in this regard. Faculty of social sciences including education department were participated in this study. Faculty teachers from multiple universities were included in this research. A simple random sampling technique was used in this regard. A questionnaire was self constructed regarding the context of teacher's awareness and its extent of usage of cybersecurity awareness, online practices, cyberbullying protection awareness, digital communication, critical thinking and cyber security risks related knowledge, strategies for safe and responsible online behaviour, social media risks and digital literacy related awareness and students learning. Tool was validated with the help of relevant educational experts, and also checked the reliability consistency by Cronbach alpha value. Data was collected by the participants and research data was entered in software for package of social sciences (SPSS) for get the results. Descriptive statistics including Mean, standard deviation and inferential statistics including chi square test for independent variables were used to get the results regarding teachers' awareness and its usage of these measures with in the classroom and students learning. The results revealed that there is no significant association among teachers' awareness regarding cybersecurity awareness measures for students. It is recommended to the institutions might include cybersecurity instruction in the curriculum, which would help students by giving them the tools they need to stay secure online. It is also proposed the heads to access cybersecurity training programs within the institutions for teachers' awareness.

***Keywords:*** Cybersecurity awareness**,** digital literacy, security risks, safety practices social media**,** cognitive abilities, phycological well- being

## INTRODUCTION

Cybersecurity awareness is a crucial competency that enables students to maintain safety and security in the online environment, safeguard their personal data, and cultivate responsible digital citizenship. This is a huge skill that is going to help students learn how to stay safe and secure online from the threat of cyber security, but also teach them how to protect their personal information in addition to developing responsible digital citizens. With an increase in reliance on technology, the cybersecurity threat is also becoming more widespread and effective. Cybercrime can have costly effects, including lost revenue, damage to reputation, and even physical injury. This is why it is important for everyone to know the risks of cybersecurity and how they can keep themselves and their information safe on the Internet. This is a digital era, wherein our personal & professional lives over lap and mingle on the internet. With almost everyone being online, having access to technology and spending their days glued to their phones it makes it easier than ever for hackers. With proper security awareness training and cybercrime protection programs, organizations can safeguard against the rising tide of emerging cybercrime. Cyber-attacks also tend to attack students, specifically the student community. Youngsters are usually less informed and more resource constrained in ensuring protection from cyberspace threats and are likely frequent users of technology for both academic and personal use. In addition, the students' inability to know and implement cybersecurity intricacies result in dire educational consequences such as leaks in data which lead to academic dishonesty (National Cyber Security Alliance 2018).

Given the increasing cyber-related risks to students' educational performance and individually understanding of cybersecurity awareness and academic outcomes needs a closer examination. The rapidly changing and sophisticated nature of cyber threats calls for a broad and holistic stance on cybersecurity education. Hobel & Huber (2019), Exploring the area of cybersecurity awareness and learning outcomes in students provides feedback to guide the development of effective strategies and meaningful programs. This is important, as these initiatives prepare students to not only protect themselves from cyber threats but also strengthen their educational goals and ambitions. This research is also of utmost importance in preparing the youth to be responsible digital citizens that will raise competent, Individuals who are empowered better steer the complexities of virtual reality while developing educationally and individually amidst this technological age that constantly reshapes our education landscape.

Many programs have been introduced by the Davao City Cyber Security Council (DCCSC) to build students awareness on technology-related risks and threats along with skills and knowledge in keeping safe online.

The latest modern technologies have changed our life like anything; especially the way information is used in various channels and how people interact with each other instantaneously (Akram et al., 2021, 2022). Around the world, people have developed different methods of communicating (Ma et al., 2025). Therefore, various agencies and also private companies have started to take up additionally solutions and advanced technologies to provide the consumer an on-demand accessibility to information at any time and anywhere (Akram & Abdelrady, 2023, 2025). Providing automated services and using innovative technologies plays an important role in catering to the needs of a multitude of customers, whose numbers are simply growing by leaps and bounds due to the rapid increase in usage of the Internet (Abdelrady et al., 2025). As a result, higher education is time and again an appealing target for many arrangements to capture academic resources via these cyberattacks in the digital age where confidentiality integrity and availability are at stake. As many students become more reliant on digital tools and online platforms for learning and administration (Jalalzai et al., 2025), they are still largely unaware of the best practices of cybersecurity (Chen & Ramzan, 2024). By not being aware of such security implications, personal and academic data of the students are exposed to being at risk — eventually jeopardising academic performance and disrupting the learning environment as a whole. This paper aims at analysing the correlation between awareness for cyber security in higher education and success of students to achieve learning cycles, reinforcing that equal cybersecurity literacy is extenuated for a safe and effective learning environment.

**Problem of the Statement**

Cybersecurity awareness is essential so that students can safeguard themselves and their information, and foster good digital citizenship. Blended learning, or the integration of digital learning in education has intensified, particularly during the COVID-19 pandemic (Younis et al., 2022; 2025). But a large number of students are still unable to demonstrate the required competencies to effectively secure themselves in cyberspace. A national survey conducted in 2020 by the Philippine National Privacy Commission showed that even amongst grade 4 students enrolled in public institution, possessed satisfactory levels of understanding about data privacy and data security (Bajo, 2020).

In the digital age, students significantly depend on online platforms for their learning. Nevertheless, a lack of awareness regarding cybersecurity measures puts them at risk of threats such as cyberbullying, phishing, identity theft, and digital distractions. These risks are not only compromising their safety but also impact their motivation, self-regulation, cognitive load, and overall academic performance. From an educational psychology view point, it is essential to investigate how increasing awareness of cybersecurity can enhance students' psychological well-being, promote self-efficacy in digital learning, and improve their academic performance.

**Objectives of the study**

This study was carried out with the following objectives:

- To find out the perceptions of teachers regarding cybersecurity awareness measures;

- To analyse the extend to which teachers implement cybersecurity awareness measures and their impact on students learning

**Research Questions**

- What are the perceptions of teachers regarding cybersecurity awareness?
- What are the levels of extend to which teachers implement cybersecurity awareness measures and their impact on students learning?

**Research Hypothesis**

**H1:** There is significant association between teachers' level and their usage of extent regarding cybersecurity awareness and students learning

**H2:** There is significant association between teachers' level and their usage of extent regarding online safety practices and students learning

**H3:** There is significant association between teachers' level and their usage of extent regarding cyberbullying protection and students learning

**H4:** There is significant association between teachers' level and their usage of extent regarding digital communication for teachers and students.

**H5:** There is significant association between teachers' level and their usage of extent regarding critical thinking about cyber security risks for teachers and students.

**H6:** There is significant association between teachers' level and their usage of extent regarding develop practices for promoting safe and responsible use of technology for teachers and students.

**H7:** There is significant association between teachers' level and their usage of extent regarding social media risks for teachers and students

**H8:** There is significant association between teachers' level and their usage of extent regarding digital literacy for teachers and students

## SIGNIFICANCE OF THE STUDY

Higher education is time and again an appealing target for many arrangements to capture academic resources via these cyberattacks in the digital age where confidentiality integrity and availability are at stake. As many students become more reliant on digital tools and online platforms for learning and administration, they are still largely unaware of the best practices of cybersecurity. By not being aware of such security implications, personal and academic data of the students are exposed to being at risk — eventually jeopardising academic performance and disrupting the learning environment as a whole. This paper aims at analysing the correlation between awareness for cyber security in higher education and success of students to achieve learning cycles, reinforcing that equal cybersecurity literacy is extenuated for a safe and effective learning environment.

**Delimitations**

• Scope: This research is only focus regarding cybersecurity awareness and the academic performance of students. Factors such as teaching methodologies, socio-economic status, or institutional resources are not considered.

• Academic Level: The study is restricted to undergraduate students (BS level) only. Students from other academic levels are not included

Institutions: This research is limited to specific higher education institutions, which means that the results may not be applicable to all universities or colleges.

## LITERATURE REVIEW

### Cybersecurity Awareness

Cybersecurity awareness is essential so that students can safeguard themselves and their information, and foster good digital citizenship. Blended learning, or the integration of digital learning in education has intensified, particularly during the COVID-19 pandemic. But a large number of students are still unable to demonstrate the required competencies to effectively secure themselves in cyberspace. A national survey conducted in 2020 by the Philippine National Privacy Commission showed that even amongst grade 4 students enrolled in public institution, possessed satisfactory levels of understanding about data privacy and data security (Bajo, 2020).

### Knowledge of Online Safety Practice

Through the use of Internet, or the World Wide Web, as it was fondly known in the beginning, a new world opened up. More than the earlier generations, we have access to information about anything with just a click. Today one can find a job, check their bank accounts, arrange vacations and trips, communicate or video chat with friends and relatives, order books, and do online shopping buying and selling products. As the number of young children on the internet and social media continues to rise, so do concerns regarding the potential risks involved in their use. Online safety or digital safety is turning out to be key especially for children nowadays (Al-Adwan et al., 2022). Safety includes a broad spectrum of issues, such as protection of personal information, cyberbullying, exposure to violence and graphic imagery, meeting strangers on the internet, and obscene language (Zilka, 2017).

## THEORETICAL FRAMEWORKS

### Cybersecurity Awareness Concepts

Understanding for cybersecurity is essential to creating and putting into practice good cyber hygiene procedures both inside businesses and among individual users. Knowledge, attitudes, and behaviors are the three primary areas into which the fundamental ideas of cybersecurity awareness can be divided (Alshaikh, Naseer, Ahmad, & Maynard, 2019; Corallo, Lazoi, Lezzi, & Luperto, 2022; Hong et al., 2023; Khader, Karam, & Fares, 2021; Li et al., 2019).

**1. Knowledge:** This dimension is interested in the knowledge and information that people possess regarding cybersecurity threats, risk handling, and countermeasures. Knowledge is what enables the cyber space to decide and assess risks. Knowledge is referring to different forms of cyber threats (e.g., malware, phishing, ransomware), attack strategies, and likely consequences of breaches.

**2. Attitude:** Attitudes towards cybersecurity determine personal beliefs and perspectives that drive an individual's position with regard to the value and efficacy of cyber hygiene measures. Favourable attitudes towards cybersecurity may motivate active participation in security programs. Unfavourable attitudes, on the other hand, can result in complacency or ignoring of advised practices.

**3. Behaviors:** are the physical things that the individual does to safeguard themselves against cyber attacks. They include the use of powerful, distinct passwords, enabling two-factor authentication, updating software regularly, and staying away from suspicious attachments or links. Behavior modification is usually the most significant objective of cybersecurity awareness training as behavior has a direct influence on people's and organizations' security stance.

**Ability to Recognize Common Cyber Threats**

Earning reassurance cyber awareness for earners is the ability to identify common cyber threats. This comprises their comprehension of certain online risks and dangers like phishing, malware, and cyberbullying. As reported by Livingstone & Haddon (2019) studied children's usage of internet technology and online experiences in Europe with a focus on their knowledge of online threats and applied safety measures. The ability to target common cyber threats is of practical significance in evaluation of cyber security awareness. A controlled study directed at learners on cybersecurity matters can be beneficial in this effort as well

**Significances of Cybercrime**

Other significant parameters of cyber security education among the learners is their comprehension of the effect of cyber crime as a Social challenge we can all relate to. Here they refer to the understanding of the harm, which cyber criminals can inflict upon an individual, an organization or society in general. Park & Kim (2018) examined South Korean students' cyber security education in relation to the students' knowledge on crime cyber crime consequences.

**Use of Secure Online Practices**

One key measure of students' awareness of cybersecurity is their employment of safe online activities. This incorporates their capacity to employ safety techniques, like making strong passwords, utilizing two-factor authentication, and staying away from dubious links, to safeguard themselves online. Students' ability to employ secure online practices and protect their personal information online was improved by cybersecurity education that used two-factor authentication and discouraged dangerous online behaviour (Madanayake et al., 2020).

**Willingness to Report Suspicious Activity**

Being willing to alert authorities or trusted people, such parents or teachers, to suspect online behaviour and cyberthreats is crucial. Wang and colleagues (2020) looked into how well a cybersecurity education program worked to increase students' propensity to report instances of cyberbullying. People who were more eager and digitally literate were more likely to report instances of cyberbullying and ask for assistance from authorities or trusted adults (Lin et al., 2023).

**Critical Thinking in the Assessment of Cybersecurity Risks**

This involves having the capacity to assess and analyse the possible dangers and hazards connected to online activities and to make well-informed choices to safeguard oneself. Cybersecurity risks and critical thinking abilities assessing online hazards and making well-informed decisions to protect oneself online, according to Lee and colleagues (2019) enhancing pupils' critical thinking abilities while keeping them safe online. Cyber hygiene and critical thinking abilities were associated with a higher likelihood of engaging in safe online behaviour, such as creating strong passwords and avoiding dubious links (Kujala et al. 2021). Assessing cybersecurity risks via critical thinking is a crucial learning objective for students. Students' critical thinking abilities can be enhanced by formal education in digital literacy and cybersecurity in the scenario of online safe measures.

**Developing Strategies for Safe and Responsible Online Behaviour**

One of the key educational results for students is the development of safe and responsible online behaviour skills. This includes learning how to identify and steer clear of harmful online behavior as well as how to protect oneself and others online. Online safety and self-efficacy are responsible for students' online behaviour, according to Gutiérrez et al. (2021). Students who had higher levels of online safety self-efficacy were more likely to use secure passwords and refrain from risky online activities, among other safe and responsible online behaviors. Formal education in digital citizenship and cybersecurity can help students become more adept at identifying and avoiding harmful online behavior as well as creating safe and responsible behavior practices with the help of online resources.

**Using of Online Resources**

The use of digital resources responsibly and ethically, which includes referencing sources and upholding intellectual property rights. The impacts of a online citizenship education program on the moral and responsible use of online resources, encompassing subjects like digital safety and respect for intellectual property rights, were examined by Neumann et al. (2018). Yıldız et al. (2022) looked at the connection between teaching students' online resources for citizenship and their ethical and responsible use of digital tools and resources. According to the study, students who had received instruction in digital citizenship were more likely to utilize digital tools and resources responsibly and ethically, including by properly citing sources and upholding intellectual property rights.

**Synthesis**

According to the literature, cyber attacks and safeguarding sensitive data require cybersecurity awareness. Various studies show that cybersecurity knowledge is positively correlated with better educational outcomes, including higher levels of academic integrity and better academic performance. Low level of cybersecurity awareness, on the other hand, is associated with a higher vulnerability to cyberattacks, which can lead to identity theft, compromised data, and academic dishonesty. It is essential to include cybersecurity education in the curriculum and give students the tools and resources they need to become more conscious of cybersecurity given the growing usage of technology in the classroom. Therefore, it is the duty of educational institutions to give cybersecurity education and awareness top priority in order to guarantee that students have the skills they need to secure their information and themselves online.

**Theories Regarding Training Program**

Theoretical bases of cybersecurity training curricula are borrowed from successful education theories, each providing a different view of what learning is and how it must be delivered.

**1. Behaviourist:** Behaviorism is concerned with observable variation in behavior caused by learning and reinforcement and external stimulus are central. Behaviorist techniques in cybersecurity training could include the application of positive reinforcement for positive security practices (e.g., completing training modules and recognizing mock phishing emails) to strengthen desired behaviors (Bush, 2006; Rogti, 2021).

**2. Cognitive Theories:** Cognitive theories are focused on psychological processes of learning, including thought, memory, and problem-solving. Cognitive theory-based security training programs try to improve the learners' knowledge and memory of security material by presenting information in an orderly fashion and exposing them to content that allows reasoning and application (Forero, 2016).

**3. Constructivist Theories**: Constructivism argues that learners build their understanding of the world and knowledge from experience and contemplation of experience. Constructivist instruction calls for students in cybersecurity to partake in experiential learning, simulations, and scenario studies with an opportunity to deepen their understanding of cyber threats and defences through active exploration and problem-solving (Daimi & Francia III, 2020; Κατσαντώνης, 2021).

## METHODOLOGY

Descriptive research design was used in this study. quantitative research method was used in this regard. The main purpose of the study was to find out the perceptions of teachers regarding need, awareness and extent level and usage for cybersecurity knowledge within the classroom and students learning. Descriptive research design was used in this study. Research survey was used in this regard. Faculty of social sciences including education department from various universities were participated in this study. Multiple university teachers frin this research. A simple random sampling technique was used in this regard. A questionnaire was self constructed regarding the context of teacher's awareness and its extent of usage of cybersecurity awareness, online practices, cyberbullying protection awareness, digital communication, critical thinking and cyber security risks related knowledge, strategies for safe and responsible online behaviour, social media risks and digital literacy related awareness and students learning. Tool was validated with the help of relevant educational experts, and also checked the reliability consistency by Cronbach alpha value. Data was collected by the participants and research data was entered in software for package of social sciences (SPSS) for get the results. Descriptive statistics including Mean, standard deviation and inferential statistics including chi square test for independent variables were used to get the results regarding teachers' awareness and its usage of these measures with in the classroom
and students learning.

## RESULTS

**Analysis: Objective 1**

| | | | | | |
|---|---|---|---|---|---|
| | **N** | **Minimum** | **Maximum** | **Mean** | **Std. Deviation** |

| | | | | | |
|---|---|---|---|---|---|
| Do you know about the cybersecurity awareness? | 25 | 1.00 | 3.00 | 2.2667 | .70373 |
| Do you know about online Safety Practices? | 25 | 1.00 | 3.00 | 1.8667 | .51640 |
| Do you know regarding cyberbullying protection? | 25 | 1.00 | 2.00 | 1.2000 | .41404 |
| Do you know about digital communication? | 25 | 2.00 | 3.00 | 2.2000 | .41404 |
| Do you know about critical thinking of cyber security risks | 25 | 1.00 | 2.00 | 1.4000 | .50709 |
| Do you know regarding develop practices for promoting safe and responsible use of technology for students? | 25 | 1.00 | 3.00 | 1.8667 | .63994 |
| Do you know about social media risks? | 25 | 2.00 | 3.00 | 2.4000 | .50709 |
| Do you know about Digital literacy? | 25 | 2.00 | 3.00 | 2.4000 | .50709 |

The table results (Mean 2.2667) and (SD 0.70373) regarding cybersecurity awareness reveal that teachers' awareness level is not very high they should get more knowledge/ awareness in this regard. (Mean 1.8667) and (SD 0.51640) results regarding online safety practices reveal that teachers are not well aware about regarding this cybersecurity measure. According to mentioned results teachers' awareness level is not very high they should get more knowledge/ awareness in this regard. (Mean 1.2000) and (SD 0.41404) results regarding cyberbullying protection reveal that teachers are not well aware about the said cybersecurity measure. Teachers generally lack sufficient awareness of measures or strategies for protecting against cyberbullying. They need to know about how educate the students about the harmful consequences of cyberbullying and provide them with strategies to prevent them from harmful consequences and can improve the students' learning. (Mean 2.2000) and (SD 0.41404) results regarding digital communication reveal that teachers are aware about digital communication knowledge but they need to get more knowledge how they can support students learning feedback, assessment as well as lifelong learning and professional development. It can also help to develop students' skills as critical thinking, problem solving and digital literacy. (Mean 1.4000) and (SD 0.50709) results regarding critical thinking about cybersecurity risks reveal that teachers are not well aware about mentioned measure. Critical thinking helps in understanding the potential impact of different cyber security risks. Critical thinking is crucial in cyber security for problem solving risks, assessment, threat detection, decision making and continuous learning. (Mean 1.8667) and (SD 0.63994) results regarding develop practices for promoting safe and responsible use of technology for the students reveal that teachers are not well aware about said measures. Digital literacy helps is to manage students' awareness regarding use of internet safely for educational purposes, responsibly and effectively. (Mean 2.4000) and (SD 0.50709) results regarding social media risks reveal that teachers are aware about the knowledge of social media risks but they need to get more knowledge regarding this said measure. Students may come across inaccurately or false information on social media, which can negatively impact on their learning outcomes. (Mean 2.4000) and (SD 0.50709) results regarding digital literacy reveal that teachers are aware about the mentioned measures, and help the students to obtain information as they need to learn and improve critical thinking skills and communication skills. E books, E learning are more effective for students innovative thinking and for educational tasks.

**Analysis: Objective 2**

**Table 1:** Teacher's awareness regarding cybersecurity

| **Chi-Square Test** | | | |
|---|---|---|---|
| | **Value** | **df** | **Asymptotic Significance (2-sided)** |
| Pearson Chi-Square | 30.000[a] | 28 | .363 |
| Likelihood Ratio | 25.597 | 28 | .595 |
| Linear-by-Linear Association | .706 | 1 | .401 |

The p-value (0.363) is greater than the significance level (e.g., 0.05). This mean there is no significant association between teachers' awareness and cybersecurity awareness. The results rejected the alternate hypothesis. While cybersecurity awareness is very effective strategy to increase the students' learning within classroom. So that's the results suggest further training or educational initiatives might be necessary to enhance cybersecurity awareness among teachers.

**Table 2:** Teacher's awareness regarding online safety practices

| Chi-Square Tests | | | |
|---|---|---|---|
| | **Value** | **df** | **Asymptotic Significance (2-sided)** |
| Pearson Chi-Square | 30.000[a] | 28 | .363 |
| Likelihood Ratio | 28.508 | 28 | .438 |
| Linear-by-Linear Association | .075 | 1 | .784 |

The p-value (0.363) is greater than the significance level (e.g., 0.05). This mean there is no significant association between teachers' awareness and online safety practices. The results rejected the alternate hypothesis. While cybersecurity awareness is very effective strategy to increase the students' learning within classroom. Teachers need to get knowledge about how they can help from emerging technologies to improve students learning. Teachers may implement home monitoring tools to help and observe students' behavior. It can also be possible with the help of learning management system (LMS) to secure and provide online practices for the improvement of the students learning. So that the results suggest that the need for training programs to improve

**Table 3:** Teacher's awareness regarding cyber bullying protection

| Chi-Square Tests | | | |
|---|---|---|---|
| | **Value** | **df** | **Asymptotic Significance (2-sided)** |
| Pearson Chi-Square | 30.000[a] | 28 | .363 |
| Likelihood Ratio | 32.556 | 28 | .252 |
| Linear-by-Linear Association | 1.813 | 1 | .178 |

The p-value (0.363) is greater than the significance level (e.g., 0.05). This mean there is no significant association between teachers' awareness and cyberbullying protection. The results rejected the alternate hypothesis. Teachers should talk with students about safe, respectful and responsible online behavior and should monitor technology and social media use in this regards, contrary no association between teachers uses and their extent regarding said measure. So that, the results suggest that teachers critical need for awareness campaigns or training programs specifically focused on cyberbullying prevention and protection strategies.

**Table 4:** Teacher's awareness regarding digital communication knowledge in classroom

| Chi-Square Tests | | | |
|---|---|---|---|
| | **Value** | **df** | **Asymptotic Significance (2-sided)** |
| Pearson Chi-Square | 30.000[a] | 28 | .363 |
| Likelihood Ratio | 29.725 | 28 | .376 |
| Linear-by-Linear Association | 2.885 | 1 | .089 |
| | | | |

The p-value (0.363) is greater than the significance level (e.g., 0.05). This mean there is no significant association between teachers' awareness and digital communication. The results rejected the alternate hypothesis. Teacher should be able to use digital tools in their classroom. Teachers should also be able to teach students digital skills like communication and critical thinking. In this regard, these skills are helpful to make an effort to listen the lesson attentively and respond appropriately against teachers questioning. This can be very helpful for students to develop content creation abilities among students. So that the results suggest that training programs might help bridge the gap and foster more advanced digital communication skills.

**Table 5:** Teacher's awareness regarding critical thinking and cybersecurity risks related knowledge

| Chi-Square Tests | | | |
|---|---|---|---|
| | **Value** | **df** | **Asymptotic Significance (2-sided)** |
| Pearson Chi-Square | 30.000[a] | 28 | .363 |

| | | | |
|---|---|---|---|
| Likelihood Ratio | 29.103 | 28 | .407 |
| Linear-by-Linear Association | 1.480 | 1 | .224 |

The p-value (0.363) is greater than the significance level (e.g., 0.05). This mean there is no significant association between critical thinking and cybersecurity risks. The results rejected the alternate hypothesis. Teachers can help the students to perform the educational tasks more efficiently and effectively. The study results indicate that students can get in-depth understanding for real word problem decision making and also be very supportive for student regarding for student's secure data, laptop security etc. for syllabus content. That's why teachers should get more knowledge regrading said measure. So that the results suggest that trainings are the necessary part to aware the teachers regarding critical thinking of cyber security risks.

**Table 6:** Teacher's awareness regarding develop practices for promoting safe and responsible use of technology

| Chi-Square Tests | | | |
|---|---|---|---|
| | **Value** | **df** | **Asymptotic Significance (2-sided)** |
| Pearson Chi-Square | 30.000[a] | 28 | .363 |
| Likelihood Ratio | 29.103 | 28 | .407 |
| Linear-by-Linear Association | .105 | 1 | .746 |

The p-value (0.363) is greater than the significance level (e.g., 0.05). This mean there is no significant association between teachers' awareness and practice for promoting safe and responsible use of technology for students. The results rejected the alternate hypothesis. In this regard, Teachers are not well aware for the knowledge for secure passwords. They should train about the strategies for use of strong password, be aware of online risks and the use of secure connection of internet. These strategies are more supportive for keep the student's education related data secure and for students effective learning. So that's the results suggest that teachers training is the necessary part to provide knowledge regarding said measure.

**Table 7:** Teacher's awareness regarding social media risks

| Chi-Square Tests | | | |
|---|---|---|---|
| | **Value** | **df** | **Asymptotic Significance (2-sided)** |
| Pearson Chi-Square | 15.000[a] | 14 | .378 |
| Likelihood Ratio | 20.190 | 14 | .124 |
| Linear-by-Linear Association | .500 | 1 | .480 |
| N of Valid Cases | 25 | | |

The p-value (0.363) is greater than the significance level (e.g., 0.05). This mean there is no significant association between teachers' awareness and social media. The results rejected the alternate hypothesis. This is the responsibility of the teachers to equipped the students with critical thinking skills for the students learning. This is the duty of teachers to provide education to those students who are social media addicted. This can lead to anxiety, depression and other mental health issues also effect on students learning success. While using social media they may have trouble paying attention in class, miss assignments and poor academic learning success. So that the results suggest teachers training must be the part in the institution.

**Table 8:** Teacher's awareness regarding digital literacy

| Chi-Square Tests | | | |
|---|---|---|---|
| | **Value** | **df** | **Asymptotic Significance (2-sided)** |
| Pearson Chi-Square | 30.000[a] | 28 | .363 |
| Likelihood Ratio | 32.556 | 28 | .252 |
| Linear-by-Linear Association | .140 | 1 | .708 |

The p-value (0.363) is greater than the significance level (e.g., 0.05). This mean there is no significant association between teachers' awareness and digital literacy for students. The results rejected the alternate hypothesis. Teachers should supportive agent for implementing critical skills in critically evaluating information of the students. Digital knowledge is very important students as well as teachers. This is the important measure. So that,

the results suggest that teachers should get more knowledge regarding this context, in this regard, teachers training is necessary part to learn more.

## DISCUSSION

Students' awareness of the dangers and hazards of technology use is becoming more and more important as a result of the expanding use of digital technologies in the classroom (Li & Akram, 2023, 2024). A crucial ability that can help kids stay safe and secure online, safeguard their personal data, and cultivate responsible digital citizenship is cybersecurity awareness. Cybersecurity awareness is the level of understanding of internet users about the importance of information security; the responsibilities and actions of internet users to implement information security controls efficiently to protect the organization's data and networks (Shaw et al. 2009). Good digital citizens understand how to use the internet and other digital technologies responsibly and ethically (Ramzan et al., 2025, 2023). They are aware of the opportunities and risks of online activities, such as accessing inappropriate content, harassment, and cybercrime). Neumann et al. (2018) investigated how a program for teaching digital citizenship affected the moral and responsible use of digital tools and resources, covering subjects like respect for intellectual property rights and online safety.

Therefore, it is the duty of educational institutions to give cybersecurity education and awareness top priority in order to guarantee that students have the skills they need to secure their information and themselves online. Online safety or digital safety is turning out to be key especially for learners nowadays. Safety includes a broad spectrum of issues, such as protection of personal information, cyberbullying, exposure to violence and graphic imagery, meeting strangers on the internet, and obscene language (Zilka, 2017).

Security and privacy of online practices incorporate students' capacity to employ safety techniques, like making strong passwords, utilizing two-factor authentication, and staying away from dubious links, to safeguard themselves online. Students' ability to employ secure online practices and protect their personal information online was improved by cybersecurity education that used two-factor authentication and discouraged dangerous online behaviour (Madanayake et al., 2020).

On the basis of literature studies cybersecurity knowledge is positively correlated with better educational outcomes, including higher levels of academic integrity and better academic performance. Low level of cybersecurity awareness, on the other hand, is associated with a higher vulnerability to cyberattacks, which can lead to identity theft, compromised data, and academic dishonesty. It is essential to include cybersecurity education in the curriculum and give students the tools and resources they need to become more conscious of cybersecurity given the growing usage of technology in the classroom. Therefore, it is the duty of educational institutions to give cybersecurity education and awareness top priority in order to guarantee that students have the skills they need to secure their information and themselves online.

## CONCLUSIONS

Cybersecurity awareness is essential for fostering a secure and resilient learning environment in higher education, directly impacting students' academic success. As digital tools and online resources become increasingly integrated into education, students are exposed to a growing range of cyber threats that can disrupt their learning processes, compromise their personal information, and even affect institutional security. By prioritizing cybersecurity awareness programs, higher education institutions empower students with essential skills to recognize, prevent, and respond to cyber threats. Moreover, equipping students with cybersecurity knowledge promotes digital literacy and responsible online behaviour, skills that are invaluable in both academic and professional settings. Enhanced cybersecurity awareness not only protects students' personal data but also helps create a culture of safety and responsibility within academic communities. Ultimately, integrating cybersecurity instruction in the curriculum supports students' learning success by enabling them to navigate and leverage digital tools with confidence and security, ensuring a safer, more productive educational experience.

**Recommendations**

On the basis of the scientific investigation this study suggests the following recommendations;

- To include cybersecurity instructions in the curriculum, providing students with the necessary tools to stay secure online.
- To provide access to cybersecurity training programs within institutions for teachers.
- For students, it is important to stay informed about online safety and responsible digital behaviour in order to benefit from a safer online experience. They should seek knowledge from trusted sources and exercise caution when sharing information.
- It is recommended that teachers develop awareness of strategies for promoting safe and secure online behavior among students.
- It is proposed that institutions develop media risk education programs to enhance students' learning and digital resilience.

## REFERENCES

1. Abdelrady, A. H., Ibrahim, D. O. O., & Akram, H. (2025). Unveiling the Role of Copilot in Enhancing EFL Learners' Writing Skills: A Content Analysis. *World Journal of English Language, 15*(8), 174-185.
2. Akram, H., & Abdelrady, A. H. (2023). Application of ClassPoint tool in reducing EFL learners' test anxiety: an empirical evidence from Saudi Arabia. *Journal of Computers in Education*, 1-19.
3. Akram, H., & Abdelrady, A. H. (2025). Examining the role of ClassPoint tool in shaping EFL studensts' perceived E-learning experiences: A social cognitive theory perspective. *Acta Psychologica, 254,104775*.
4. Akram, H., Abdelrady, A. H., Al-Adwan, A. S., & Ramzan, M. (2022). Teachers' perceptions of technology integration in teaching-learning practices: A systematic review. *Frontiers in psychology*, *13*, 920317.
5. Akram, H., Yingxiu, Y., Al-Adwan, A. S., & Alkhalifah, A. (2021). Technology Integration in Higher Education During COVID-19: An Assessment of Online Teaching Competencies Through Technological Pedagogical Content Knowledge Model. *Frontiers in Psychology*, 12, 736522-736522.
6. Al-Adwan, A. S., Nofal, M., Akram, H., Albelbisi, N. A., & Al-Okaily, M. (2022). Towards a sustainable adoption of e-learning systems: The role of self-directed learning. *Journal of Information Technology Education: Re-search, 21,* 245-267.
7. Alayo, J. G., Mendoza, P. N., Armas-Aguirre, J., & Molina, J. M. (2021). Cybersecurity maturity model for providing services in the financial sector in Peru. In *2021 Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI)* (pp. 1-4). IEEE.
8. Alshaikh, M., Naseer, H., Ahmad, A., & Maynard, S. B. (2019). Toward sustainable behaviour change: an approach for cyber security education training and awareness.
9. Bajo, J. C. (2020). Data privacy awareness of public-school students in PH at 4% - study. ABS-CBN News. https://news.abs-cbn.com/news/11/19/20/data-privacy-awareness-of-public-school-students-in-ph-at-4-study
10. Bush, G. (2006). Learning about learning: From theories to trends. *Teacher Librarian, 34*(2), 14.
11. Chen, Z., & Ramzan, M. (2024). Analyzing the role of Facebook-based e-portfolio on motivation and performance in English as a second language learning. *International Journal of English Language and Literature Studies*, *13*(2), 123-138.
12. Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry, 137*, 103614.
13. cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13-24.
14. Daimi, K., & Francia III, G. (2020). *Innovations in cybersecurity education* (Vol. 388): Springer.
15. Forero, C. A. M. (2016). Tabletop exercise for cybersecurity educational training; theoretical
16. grounding and development. *MS Thesis*.
17. 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
18. Hu, T., Wang, K. Y., Chih, W., & Yang, X. H. (2020). Trade off cybersecurity concerns for co-created value. *Journal of Computer Information Systems*, *60*(5), 468-483.
19. Jalalzai, N. N., Akram, H., Khan, M., Kakar, A. K. (2025). Technology Readiness in Education: An Analysis of ICT Facilities in High Schools of Loralai, Balochistan. *Contemporary Journal of Social Science Review*, 3(3), 2835-2842.
20. Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information, 12*(10), 417.
21. Krombholz, K., Hobel, H., & Huber, M. (2019). Cybersecurity education: The need for a holistic and integrated approach. *Communications of the ACM, 62(8), 48-54.*
22. Kujala, M., Ronkainen, J., & Tebest, T. (2021). Critical thinking skills and cyber hygiene practices among primary school pupils in Finland. *Journal of Information Security and Applications, 58, 102769. doi: 10.1016/j.jisa.2021.102769*
23. Lee, Y. H., Lee, H. J., & Ahn, C. K. (2019). The effects of cybersecurity education on critical thinking skills in fourth-grade students. Journal of Educational Technology, 35(4), 825-841. doi: 10.17232/KSET.35.4.825
24. Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of
25. Li, S., & Akram, H. (2023). Do emotional regulation behaviors matter in EFL teachers' professional development?: A process model approach. *Porta Linguarum: revista internacional de didáctica de las lenguas extranjeras*, (9), 273-291.
26. Li, S., & Akram, H. (2024). Navigating Pronoun-Antecedent Challenges: A Study of ESL Academic Writing Errors. *SAGE Open*, *14*(4), 21582440241296607.
27. Livingstone, S., & Haddon, L. (2019). EU Kids Online: Final report. London, UK: London School of Economics and Political Science. Retrieved from http://eprints.lse.ac.uk/24313/
28. Ma, D., Akram, H., & Chen, I. H. (2024). Artificial Intelligence in Higher Education: A Cross-Cultural Examination of Students' Behavioral Intentions and Attitudes. *The International Review of Research in Open and Distributed Learning*, *25*(3), 134-157.
29. Madanayake, B. L., Samarawickrama, P. S., & Hewagamage, K. P. (2020). Effectiveness of a cybersecurity education programme on the online safety practices of primary school students in Sri Lanka. Education and Information Technologies, 25, 4747-4765. doi: 10.1007/s10639-020-10240-2

30. National Cyber Security Alliance. (2018). Back to school: Securing the digital generation. Retrieved from https://staysafeonline.org/wp-content/uploads/2018/08/Back-to-School-Securing-the-Digital-Generation.pdf
31. Neumann, M. M., Neumann, D. L., Walker, R. A., & Baker, J. (2018). The effects of a digital citizenship program on the ethical and responsible use of technology in a rural school district. Computers in the Schools, 35(2), 95-110. doi: 10.1080/07380569.2018.1437517
32. Park, H. J., & Kim, J. (2018). The effects of cybersecurity education on elementary school students' awareness of cybercrime consequences. Journal of Educational Technology, 34(4), 617-630. doi: 10.17232/KSET.34.4.617
33. Qi, Y., Gu, Z., Li, A., Zhang, X., Shafiq, M., Mei, Y., & Lin, K. (2023). Cybersecurity knowledge graph enabled attack chain detection for cyber-physical systems. *Computers and Electrical Engineering*, *108*, 108660.
34. Ramzan, M., Akram, H., & kynat Javaid, Z. (2025). Challenges and Psychological Influences in Teaching English as a Medium of Instruction in Pakistani Institutions. *Social Science Review Archives*, *3*(1), 370-379.
35. Ramzan, M., Bibi, R., & Khunsa, N. (2023). Unraveling the Link between Social Media Usage and Academic Achievement among ESL Learners: A Quantitative Analysis. *Global. Educational Studies Review, 8*, 407-421.
36. Rogti, M. (2021). Behaviorism as external stimuli: improving student extrinsic motivation through behavioral responses in algerian college education. *Global Journal of Human-Social*
37. *Science, 21*(1), 29-41.
*38.* university students and working graduates. *Education and Information Technologies,*
39. Yıldız, B., & Gejam, E. H. Y. (2022). Cyber-Physical Systems and Cyber Security: A Bibliometric Analysis. *OPUS Journal of Society Research*, *19*(45), 35-49.
40. Yıldız, R., Yıldırım, S., & Bozkurt, A. (2021). The effect of digital citizenship education on fourth grade students' ethical and responsible use of technology. Education and Information Technologies, 26(3), 2303-2319. doi: 10.1007/s10639-021-10545-y
41. Younas, M., Noor, U., Zhou, X., Menhas, R., & Qingyu, X. (2022). COVID-19, students satisfaction about e-learning and academic achievement: Mediating analysis of online influencing factors. *Frontiers in psychology*, *13*, 948061.
42. Younas, M., Ismayil, I., El-Dakhs, D. A. S., & Anwar, B. (2025). Exploring the impact of artificial intelligence in advancing smart learning in education: A meta-analysis with statistical evidence. *Open Praxis*, *17*(3), 594-610.
43. Zilka, G. C. (2017). Awareness of e Safety and potential online dangers among children and teenagers. *Journal of Information Technology Education. Research*, *16*, 319.