ACADEMIA International Journal for Social Sciences
Volume 5, Issue 2(a), 2026 ISSN-L (Online): 3006-6638

From Awareness to Protection: Investigating Cybercrime Knowledge and Victimization Risks Among Prospective Teachers

Muhammad Imran
connect2imran77@gmail.com
School Education Department, Punjab, Pakistan

Dr. Nargis Abbas
nargis.abbas@uos.edu.pk
Associate Professor, Institute of Education, University of Sargodha, Pakistan

Rizwan Abbas Nasimi
rizwannasimi1843@gmail.com
Assistant Education Officer, School Education Department Punjab, Pakistan

Corresponding Author: Muhammad Imran connect2imran77@gmail.com

Received: 13-01-2026 **Revised:** 28-01-2026 **Accepted:** 12-02-2026 **Published:** 26-02-2026

ABSTRACT

Globalization of information and communication technologies (ICT) has revolutionized education and provided new prospects in learning and professional growth. Nonetheless, with this digital development, there is also a great challenge including those concerning security. This study aimed to analyze the knowledge, awareness and risk of victims of cyber-crime among prospective teachers of public sector universities of Punjab, Pakistan. The research's focus is on how social and professional ties relate to the awareness and protective practices of cybersecurity, guided by Social Bond Theory, which suggests that close social relationships and conforming to societal norms lowers deviant behaviors. A quantitative research design was used to survey students attending various universities with a structured questionnaire to measure cyber-crime awareness, threat exposure, and use of cyber safety precautions. The reliability analysis showed that constructs measured were reliable and suitable for analysis. The results indicate that potential teachers have a moderate awareness of cyber-crime dangers and different levels of involvement in protective conducts. Increased awareness was correlated with more proactive security measures, but there is still a lack of knowledge about what to report and how to deal with social engineering threats. Overall, the findings underscore the importance of robust cyber security education initiatives within higher education institutions, particularly focusing on preventive measures and safe online practices to empower the next generation of educators to operate safely and responsibly in digital spaces.

Keywords: *Cyber-crime, Harassment, Perception about Cyber-crime, Reaction of Reporting Incident Suggestions on Cyber-crime, Reporting Mechanism*

INTRODUCTION

Globalization of information and communication technologies (ICT) has revolutionized education and provided new prospects in learning and professional growth. Nonetheless, with this digital development, there is also a great challenge including those concerning security. Financial fraud, identity theft, cyber harassment, and data breaches, all of which are classified as cybercrime, are a severe threat to the social stability and national security (Khan, 2025). Schools and universities are also most vulnerable to cyberattacks as different facets of education are increasingly dependent on digital platforms in teaching, administration and communication. This is why it is so crucial to have strong cybersecurity systems and

be more aware (Kont, 2025).

The problem of cybercrime in Pakistan is increases over time, and there is a lack of legal enforcement, technological infrastructure, and perspectives of the population (Masudi, 2023). To the future educators, it is essential to learn about and know how to deal with cyber threats, not only to keep themselves safe but also to teach their future generation how to practice cyber safety (Adey et al., 2025). The paper discusses the level of awareness on cybercrime among potential teachers in state-owned universities in Punjab, Pakistan. It seeks to point out the overwhelming demand that there is a necessity to provide better cybersecurity training to teachers in their training programs so that they may establish an educational environment that is more secure and digitally literate.

Setting in Pakistan and Punjab Universities.

The issue of cybercrime has become a big problem to many sectors in Pakistan, especially the educational sector (Adeshola and Oluwajana, 2024). Universities have become susceptible to cyber threats due to such practices as the extensive use of digital technologies in higher education as the "Smart Education" program by the Higher Education Commission (Maria et al., 2025). These dangers include theft of data, ransomware, and so on, which further increases the necessity of the extensive cybersecurity training of faculty, staff, and students (Kont, 2025).

The training of future teachers is centralized in the universities of Punjab. Although many teachers may be conversant with the fundamentals of cybersecurity, including phishing and effective passwords, they have major gaps in their implementation of effective security practices. Also, a significant number of educators mix cybersafety, which deals with safe behavior in the online environment, and cybersecurity, which deals with technical protection (Lamond et al., 2025). This misunderstanding, along with a wider systemic problem, shows why digital literacy and cybersecurity education should be reformed in Pakistani institutions of teacher training (Hockly, 2023).

Cybercrime Awareness is the knowledge an individual has in different types of cybercrime such as phishing, malware, cyberbullying, online fraud and identity theft among others. It includes awareness of how such crimes work, their possible impacts, and the ways to reduce the impact. It is also characterized by being knowledgeable of the official platforms of reporting a cyber incident where the organization can not only be aware of threats but also know what to do in cases where the threat is realized (Andria et al., 2025). To promote a culture of digital awareness, the awareness of cybercrime must be high so that the prospective teacher can be able to learn how to recognize risks and direct students to safer practices on the internet.

Digital literacy is used to determine the capacity of the potential teachers in terms of access, evaluation, creation, and sharing of information using digital tools and platforms. It encompasses more than simple technical skills and it is the skill to critically evaluate digital materials, navigate complicated online space and use technology in a responsible manner. With the growing importance of digital spaces in learning and in everyday life, a high level of digital literacy is one of the defining factors to determine the possible cyber threats and use technology as an instrument to maintain a safe and efficient learning process (Safdar et al., 2025). This competency is also fundamental in enabling the future educator to enable his or her students to engage safely and meaningfully with digital content.

Perception of cyber threats is the perceptions of the potential teachers with reference to the probability and seriousness of different cyber threats. Proactive cybersecurity behaviors are greatly motivated by a position of being well-informed about these risks. The closer people can estimate the risks of cybercrime, the higher the chances of people practicing behavior that alleviates exposure to cyber threats. This variable

shows the significance of the development of a realistic perception of cyber risks that can trigger future educators to implement the necessary precautions, including securing personal information and educating students about safe online practices (AlQarni, 2025).

The relationships between these variables are fundamental towards a complete picture of cybercrime awareness. Good level of digital literacy having a beneficial effect on cybercrime awareness since better users of digital technologies will be well prepared to understand the specifics of online threats and protection (Safdar et al., 2025). Increased cybercrime awareness, its turn, may perfect the perception of a potential teacher about cyber threat, and promote a more realistic perspective on risks and the attitude to acquire secure online practices (AlQarni, 2025).

Such knowledge gap does not only subject future educators to different personal and professional dangers, but it also compromises their capability to educate and protect their students in a more digital world. The digital security practices need to be well-known to the prospective teachers who act as role models to the future generation so that they can provide a safe and responsible online environment to their students. Regrettably, this lack of awareness on cybercrime impairs their ability to teach important online safety skills hence threatening the educational process.

Besides, the issue of the absence of formalized cybersecurity training in educator education programs also contributes to the heightened risk and vulnerability of both teachers and learners to possible cyber threats. Nevertheless, in this regard, the lack of and uneven cybercrime education and capability of would-be teachers in Punjab universities is not only a personal problem but also a systems problem that creates substantial risks to individual data security, professionalism, and the education system as a whole. The implications of the knowledge gap may be extensive, and future security of the educational settings in the region may be compromised.

This paper aimed to examine the level of awareness of cybercrime among future educators studying at the universities in the Punjab region of Pakistan in the public sector. The study will also serve to underscore the necessity of incorporating the issue of cybersecurity education within the training programs of teachers by pinpointing the major reasons that cause this lack of awareness. The lack of such knowledge will keep exposing educational institutions to high levels of vulnerability that may threaten the personal security of the teachers and students and the sustainability of the educational process. Therefore, there has never been a more pressing need than now to consider the increase in cybersecurity education and training during teacher preparation programs.

The fact that the digital technologies in the educational process are getting more and more integrated all over the world opens up enormous opportunities, yet it also poses about as many challenges as it offers, and especially in the area of cybersecurity. The growth of cybercrime in Pakistan, particularly within the education industry, has posed an increasing challenge to personal security of students and teachers, not to mention integrity of education systems. Since future teachers are the new teachers who will determine the relationship of the future generation with digital tools, it is important to evaluate their level of awareness and readiness on cyber threats. The proposed research seeks to fill this gap by investigating the present level of cybercrime awareness among the potential teachers in the Punjab region, in Pakistan, in public universities.

Although the significance of cybersecurity awareness in the educational sector is gaining recognition across the world, there is a observable lapse in the knowledge and readiness among teachers, especially in Pakistan. The study also aimed at assessing the amount of knowledge that the future teachers possess regarding cybercrime and its possible consequences not only on their own personal safety, but also on their students. Moreover, through evaluating the connection between cybercrime knowledge and

victimization, this research work seeks to draw an important attention to the significance of education in creating safe digital behaviors.

The rationale of the current study lied in the fact that there is an urgent need to provide future educators with devices and knowledge that help them to fight cyber threats not only to preserve their personal safety but also so that they would be able to share the necessary cybersecurity skills with their students. The education system of Pakistan is prone to cyber-attacks without proper training and this may have long-term consequences on teachers and learners. Therefore, the results of this study added the larger debate on how to improve cybersecurity training in teacher preparation programs that are required to provide a secure and digitally literate educational setting in Pakistan.

LITERATURE REVIEW

The increasing use of online technologies in the educational process implies the rise of the relevance of cybercrime awareness among future educators. This literature review is an overview of already known studies on cybercrime and its effects on future teachers in contemporary educational institutions. Cybercrime is a wide category of criminal activities that deal with computer systems and networks, which is a very dangerous threat to both the individual and the institution (Ibrahim and Rajalakshmi, 2025). With the digital environment growing larger and larger, the knowledge of these threats becomes more and more critical, especially in the academic environment where the interdependent nature of systems and the culture of open access makes it more vulnerable (Ibrahim and Rajalakshmi, 2025).

Learning institutions are particularly vulnerable to cyber-attacks because they use digital systems. Ransomware is among the most significant types of cybercrime, during which information of an institution is encrypted and released only under the condition of payment, which is often in cryptocurrency. These attacks interfere with academic processes, impair access to vital systems and can result in a loss of finances, reputation and legal repercussions. Universities are vulnerable areas, especially where the university has no sufficient cybersecurity protocols and backup systems (Salam et al., 2025; Olayinka, 2025).

The phishing and social engineering types of attacks pose threats as well in the educational setting. These attacks exploit individuals to reveal sensitive data like passwords and monetary information by use of misleading emails, counterfeit sites among others. They are more effective when used in the academic environment where users might be poorly trained and lack cybersecurity awareness. Using the human error and trust, rather than a technical weakness, as an entry point, such attacks can be the gateway to more serious cybercrimes, such as data breaches and ransomware cases (Ibrahim and Rajalakshmi, 2025; Salam et al., 2025).

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks are very dangerous to institutions of higher learning because they flood servers or networks with heavy traffic hence rendering services unusable by the authorized users. DDoS attacks are also hard to manage since they are distributed in nature whereby there are various sources of attack. Educational institutions, particularly universities that rely heavily on the Internet to process course applications, research partnering and to communicate, are particularly susceptible. These attacks have the capability of interrupting important services like learning management systems, websites, email servers, and databases that cause an immediate difficulty in accessing important resources by the students and faculty. Also, there is a risk of long-lasting downtime in institutions, which will lead to losses in productivity and economic harm. In other cases, the attacks can also be used as the distraction of more complicated cyber intrusions (Ibrahim & Rajalakshmi, 2025).

Another major security issue in cybersecurity is spoofing, which entails people with bad intentions posing as trusted parties to trick the users. Such common ones are email and IP spoofing; they are used to lure

people to provide sensitive information or work with hostile material. Academic institutions are the most common victims of this type of attack on students, faculty, and staff, and it takes advantage of the trust and lack of awareness. Their disingenuous character causes them to be hard to trace and may attract more severe repercussions like breach of data and frauds. To mitigate it, it is needed to strengthen email security, multifactor authentication, and user awareness (Ibrahim and Rajalakshmi, 2025).

Hackers and theft of data also pose a great risk to universities because sensitive information like personal records, research data, and financial information is being targeted. Such attacks may cause financial losses, legal, reputational damages, and undermined academic integrity and it is important to ensure access controls are strong, use encryption, and regularly monitored (Ibrahim & Rajalakshmi, 2025).

Sextortion is a cybercrime type whereby a person finds himself in the hands of an attacker who threatens to post sexually explicit content unless the victim meets specific requirements, usually (though not always) money or more explicit content. Such cyber-crime can destroy the victims both emotionally and psychologically especially in learning institutions, where students might be at a disadvantage. Another potential threat is open AI-giarism, which refers to the manipulation or creation of content by using tools of artificial intelligence. This may be plagiarism, stealing content, or making deceiving information with AI-based technology. Sextortion and the use of AI in manipulating content are very critical issues to academic institutions because they not only hurt people but also damage the inner workings of the educational process. With the development of AI technologies, the threat of such crimes growing is more likely, which is why it is highly important that universities learn to be aware of these threat types and create more robust protection against them (Olayinka, 2025).

Cyberbullying is an online type of harassment, and it is the type of harassment in which individuals utilize digital media to attack, intimidate, and embarrass others. It is usually the case in education, though faculty or staff may be involved in it. Cyberbullying may have a variety of forms such as intimidating emails, teasing other users by spreading rumors or publishing negative posts on social media. The impact of cyber bullying may be long-term with the consequence being anxiety, depression and deterioration of academic performance of the victim. Students in universities are active on social media and other digital communication platforms, which increases the risk of cyberbullying. Although, it is common to talk about cyber safety in most institutions there are certain learning interventions that are necessary when it comes to cyberbullying so that the students are not only informed about the dangers but also know how to report and respond to such threats. Educational centers are supposed to have clear policies in place and support systems to deal with and prevent cases of cyberbullying (Karayol et al., 2025). All these varieties of cyber threats underscore the importance of having a strong cybersecurity system and awareness training to all stakeholders in higher education (Olayinka, 2025).

The research always demonstrates an increased awareness of the role of cybersecurity in education. Most educators are conversant with the basic cybersecurity concepts. In particular, a preliminary study of cybersecurity awareness among school teachers established that although a large number of teachers were conversant with fundamental concepts and were aware of the most critical aspects, such as phishing and robust passwords, gaps remained in the real-life implementation of cybersecurity strategies (Andria et al., 2025). This implies that the conceptual awareness may not necessarily be transferred into practices of consistent protection.

The previous studies further suggest that security awareness is based on education and knowledge, which allow people to safeguard themselves against cyber-attacks (Lazarov et al., 2025). Nevertheless, there remains a significant discrepancy in the way educators define and understand cybersecurity and tend to confuse such a notion with a bigger notion, such as online safety (Childers et al., 2025). This theoretical vagueness may cause a decrease in attention to the technical components of the cybersecurity issue like

knowledge of using safe passwords and authentication systems (Lamond et al., 2025). As a result, cybersecurity education at schools tends to be somewhat sporadic, with the absence of resources and skills among teachers as some of the factors (Lamond et al., 2025). The importance of cybersecurity education to start at the primary schools up to universities and its continuity in the public and the privatized sectors is gaining more and more significance (Lazarov et al., 2025).

Despite the recent stress on cybersecurity education by the global community, the research on the level of the knowledge and awareness of future teachers in Punjab, Pakistan, is uncommon, especially in studies published since 2024. The available literature, however, points to systemic issues across the Pakistani universities that have a major impact on future educators. Educational institutions have become more vulnerable to cyber attacks due to the digital transformation of higher education, especially in programs like the Smart Education program (Maria et al., 2025). This increased exposure is added to the lack of cybersecurity awareness among students and faculty, which adds to educational system vulnerabilities and sensitive data (Bhatt & Shah, 2025).

Digital citizenship studies have also shown that there are significant gaps in the knowledge of pre-service teachers, which are culturally mediated, infrastructurally constrained, and poorly integrated into the curriculum (Safdar et al., 2025). Such shortcomings show that there are still the problems with digital literacy and cybersecurity awareness, which may impede safe and effective interactions in digital space. The same issues in the related situations, like in Saudi Arabia, highlight the greater significance of poor training and insufficient educational facilities (AlQarni, 2025).

Consciousness in cybersecurity can help with minimizing victimization because more people are aware of cybercrime, including phishing and social engineering (Madzvamuse, 2025). Moreover, awareness is a positive factor that affects protective behavior, which promotes the use of stronger data security practices (AlQarni, 2025). On the other hand, the lack of cybersecurity expertise makes people more vulnerable to cyber-attacks and the theft of personal data, which once again confirms the necessity to provide aspiring teachers with the necessary skills in digital safety (Nadiba, 2025).

There are still a number of obstacles and areas of weakness that prevent successful cybersecurity training of potential teachers in the world and in Pakistan in particular. The first obstacle is uncoordinated curricula and lack of parental participation in cybersecurity education in school systems (Long, 2025). It is also seen that teachers usually have limited resources, and they lack skills, and it is hard to incorporate effective cybersecurity education into the instruction (Lamond et al., 2025). The teachers are not ready to teach aspects of cybersecurity, and it is necessary to enhance their training and support (Lamond et al., 2025).

Moreover, swift development of cyber threats implies that learning material must be continuously renewed in order to be up to date (Long, 2025). Research indicates that in cases where teachers know the rudimentary concepts, they might experience difficulties in deploying the measures of cybersecurity, which implies that additional, more practical, and hands-on education should be implemented to overcome the challenges of an abstract understanding of the material (Andria et al., 2025). Reforming the digital learning curriculum and building sufficient digital infrastructure is essential in the context of Pakistan to eliminate the current knowledge gaps in pre-service teachers (Safdar et al., 2025). Cultural peculiarities and a lack of local research also present their own problem and make creating contextually applicable cybersecurity training programs more complicated (Safdar et al., 2025). It is also necessary to have programs that are specific to the region and consider the specific weaknesses of educators in a more digitalized world.

Research Objectives

- To assess prospective teachers' knowledge of various types of cybercrimes.

- To evaluate their awareness of cybercrime risks and prevention strategies.
- To examine the link between cybercrime knowledge and vulnerability to cyber victimization.

Theoretical Framework

The present research is supported by the Social Bond Theory, which was now firstly developed by Travis Hirschi in 1969 and suggests that the relationship of individuals with societal institutions and norms has an impact on their likelihood of committing deviant acts. The theory identifies four major components, which include attachment, commitment, involvement, and belief, indicating that the stronger the social bonds, the less likely the person is to commit a crime, which can be used to prevent crime on a community level (Dewi, 2025). This model in the modern digital environment is applied to knowing how these relationships may affect cybersecurity practices and vulnerability to cybercrime victimization.

Applying to the case of future educators, the theory posits that strong bonds to the professional community, dedication to educational values, participation in safe online behaviors and orientation towards the significance of cybersecurity standards makes them more vigilant and reduces the likelihood of unsafe online behavior (Shari, 2025). Indicatively, research has shown that e-crime can be considerable with the reinforcement of social relationships (Shari, 2025). Moreover, compliance with information security policies will be enhanced once people are closely connected with their communities (Mui et al., 2025). On the other hand, less strong social ties between potential teachers may be associated with lower cybercrime awareness and higher vulnerability as they may not be as well incorporated in a protective social system promoting cautious online habits. In this way, the Social Bond Theory is effective in addressing the question of how the social affiliation of the potential teachers, their cybercrime knowledge, and their vulnerability to becoming victims of cyberattacks in the educational contexts are linked to each other (Akter and Wiśniewski, 2025).

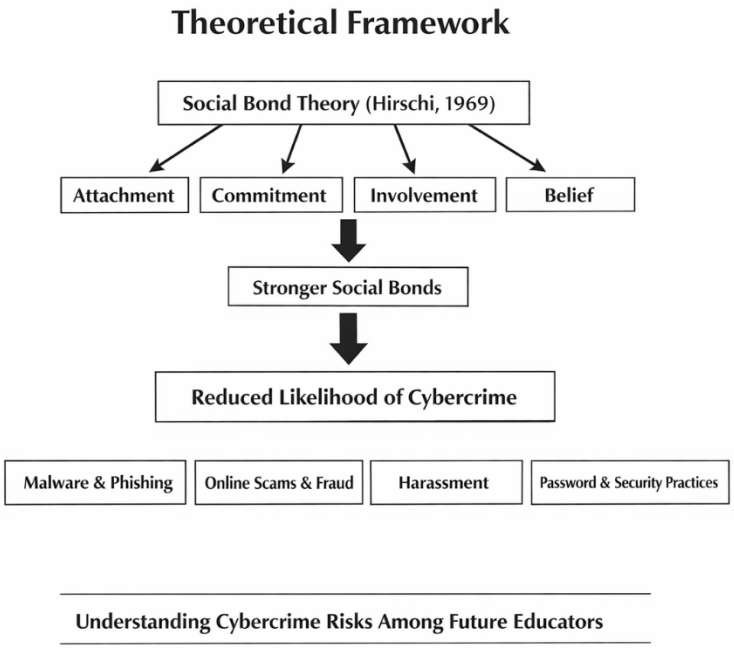

Figure.1 Theoretical framework

Conceptual Framework

The research design used in the study Cyber Crime Awareness and Its Causes Among the Prospective Teachers was to analyze the linkage between the knowledge of the prospective teachers on cyber-crimes and their susceptibility to cyber victimization. The research aimed at the cognition of how awareness of different cyber-crimes, including malware, phishing, online scams, and harassment, of the prospective teachers affected the way they recognized the risk and used prevention strategies. It aimed to analyze how knowledge of such concerns could hinder chances of being a victim of cyber-crime.

The main participants in the framework were the prospective teachers and their awareness of cyber-crime was the focus of the study. The study questions were aimed at measuring the knowledge level of the teachers regarding various forms of cybercrimes, the level of understanding the risks and the correlation between knowledge and susceptibility. The hypothesis of the framework was that, the higher the awareness, the less susceptible to cyber-attacks and stronger the understanding of prevention practices, the higher the likelihood of avoiding cyber victimization. Furthermore, the paper examined the relevance of offering precise guidelines on how to enhance the level of cyber-crime awareness among future educators, who should be highly equipped with information on how to manage any possible cyber threats in their professional and personal lives.

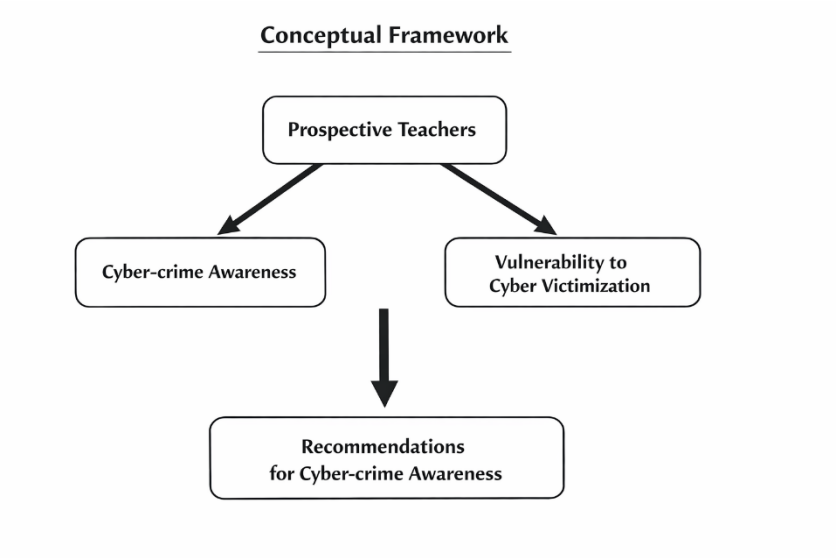

Figure.2 conceptual framework of the study

MATERIAL AND METHODOLOGY

In this study, a quantitative research design is utilized with a survey approach as the tool to evaluate the level of awareness regarding cyber-crime in potential teachers in the public universities of Punjab in Pakistan. A questionnaire was the main data collection instrument that enabled the questionnaire to be anonymous and cost-effective and collected a large amount of data. The surveys can be applied to test the theories and establish the population characteristics (Jackson, 2011). Nevertheless, there are issues that can be faced like response depth and bias that should be considered.

The research is aimed at undergraduate undergraduates of the last semester of three randomly chosen state-owned universities in University of Punjab, IUB Bahawalpur and University of Sargodha. Multi-stage

sampling was employed, whereby random sampling of universities was done after which, purposive sampling of the students of the Department of Education was done. The stratified sampling was to guarantee the representation of the 6th semester BS, 8th semester BS, and 3rd semester B.Ed. (1.5) students, where 30 percent of the students were picked. The last sample contain 300 students, aged between 18 and 26.

A researcher-designed questionnaire with 54 questions and structured on a seven-point Likert scale was used to collect the data. The content of the items is related to cyber-crime knowledge, the experience with phishing and malware, and the attitude to cybersecurity practices.

Three gurus of Sargodha University, Faisalabad University and Government College University validated the instrument. Split-half reliability was determined by use of 20 students and the Cronbach alpha coefficient was determined to be 0.88 which is a high level of reliability.

Level	Item No	Cronbach Alpha (α)
Perception of Cyber crime	**1-5**	.712
Malwares	6-10	. 735
Phishing	11-17	. 807
Online scams	18-22	. 723
Harassment	23-25	. 775
Frauds involving electronic fund transfers/ credit cards	27-30	. 578
Password usage	31-39	**.** 791
Anti-virus software	40-44	**.** 755
Social engineering	45-56	**.** 858

DATA ANALYSIS

Demographic information result showed the data regarding research participants their gender, age, University, semester and session and it is showed, whether the individuals in a particular study are a representative sample of the target population for generalization purposes.

Table 1

Demographic information of prospective teachers

Variables	Frequency	Percentage
Gender		
Male	92	33.1
Female	186	66.9
Age		
18-22	92	33.1
22-26	186	66.9
University		
SU	99	35.6
IUB	81	29.1
PU	98	35.3
Semester		
2nd	65	23.4
4th	24	8.6
6th	114	41.0
8th	75	27.0
Session		
BS 2018-22	83	29.9
BS 2019-23	53	19.1
BS 2020-24	36	12.9
B.Ed. (H) 2018-22	9	3.2

B.Ed. (H) 2019-23	28	10.1
B.Ed. (H) 2020-24	5	1.8
B.Ed. (1.5) 2020-22	32	11.5
B.Ed. (1.5) 2021-23	32	11.5

Table No 1 shows that, out of selected sample of the study, total 66.9% of the female and 33.1% of the male prospective teachers participated in the current study. The distribution of the total sample with respect to their age indicated that 33.1% prospective teachers were from age group 18-22 and 66.9% from the age group of 22-26 respectively. Further, 35.6% prospective teachers were from Sargodha University, Sargodha 29.1% Prospective teachers were from Islamia University of Bahawalpur and 35.3% prospective teachers were from Punjab University, Lahore. This table also shows the distribution of prospective teachers with respect to their semester. There were 9% prospective teachers form 2nd semester, 8.6% from 4th semester, 41% from 6th semester and 27% from 8th semester. Moreover, distribution of data with respect to their session indicated that 29.9% prospective teachers were form BS 2018-22 session, 19.9% were from BS 2019-23 session, 12.9% were from BS 2020-24 session, 3.2% were from B.Ed. (Hons) 2018-22 session, 10.1% were from B.Ed. (Hons) 2019-23 session, 1.8% were from B.Ed. (Hons) 2020-24 session, 11.5% were from B.Ed. (1.5) 2020-22 session and 11.5% were from B.Ed. (1.5) 2021-23 session.

Table 2

Mean, standard deviation and bivariate correlations between the variables

Variables	N	Mean	SD	1	2	3	4	5	6
1. PCC	278	22.0432	6.19056	1					
2. MW	278	17.3285	5.36599	0.576***	1				
3. PS	278	26.700	5.13704	.007	0.278***	1			
4. OS	278	14.6268	3.69007	0.295***	0.412***	0.122*	1		
5. HS	278	10.5487	4.73064	.296***	-.041	0.363***	-0.073	1	
6.FC	278	14.1018	4.32745	-0.60	.358***	1.425***	0.305***	0.397***	1

7.PU	278	34.6838	6.99098	0.013	.231***	0.457***	0.122*	0.463***	0.411***
8.AVS	278	19.4838	3.71404	.283***	0.377***	0.145*	0.165**	0.03	0.226***
9.SE	278	44.4835	8.45537	-0.006	0.182**	0.496***	0.135*	0.498***	0.500***

** p< 0.01 & *** p < 0.001

Table 2 shows descriptive statistics and correlation among the variables associated with cybercrimes (PCC, MW, PS, OS, HS, FC, PU) and safety measures (AVS and SE) for 278 respondents. The safety measure AVS had a mean of 19.48 (SD = 3.71), while SE showed a higher mean of 44.48 (SD = 8.46). AVS was significantly and positively correlated with PCC (r = .283, p < .001), MW (r = .377, p < .001), PS (r = .145, p < .05), OS (r = .165, p < .01), and FC (r = .226, p < .001), but showed a negligible relationship with HS (r = .030, p > .05). This suggests that there is a correlation between the factors of cybercrime and the use of or awareness of AVS safety measures. Similarly, SE was positively associated with MW (r = .182, p < .01), PS (r = .496, p < .001), OS (r = .135, p < .05), HS (r = .498, p < .001), and FC (r = .500, p < .001), while it was not significantly related to PCC (r = −.006, p > .05). The findings indicate that people who are more exposed to various cybercrime factors tend to accept and report higher use of SE safety measures. The correlations overall, though, are positive and consistent, signifying that the more involved one becomes in cybercrime related experiences, the more likely he or she will take precautions to keep safe; however, these do not necessarily mean causation.

Table 3
Regression Results: Effect of PCC on Outcome Variables

Outcome	B (SE)	β	t	p
Malware	0.50 (0.04)	0.57	11.61	***
Online Scams	0.18 (0.03)	0.30	5.30	***
Harassment	–0.07 (0.02)	–0.18	–3.00	**
Anti-Virus Software	0.36 (0.04)	0.47	8.73	***

*Significance: ***p < .001, **p < .01.*
*Malware — R^2 = 0.33, F (1,276) = 134.79****
*Online Scams — R^2 = 0.09, F(1,276) = 28.12****

*Harassment — $R^2 = 0.03$, $F(1,276) = 8.99$***
*Anti-Virus Software — $R^2 = 0.22$, $F(1,276) = 76.25$****

Table 3 gives the regression outcomes that investigate the influence of the perception of cyber-crime (PCC) on diverse outcomes, including the usage of malware, online scam, harassment, and the usage of anti-virus software. The discussion shows the role of increasing awareness of cyber-crime in changing the behaviors associated with the digital threats, which have different levels of strengths as per the outcomes. The findings indicate that the more the individuals are aware of cyber-crime, the more their potential to commit or become victims of some cyber threats varies. Regression analysis indicates that there is a positive moderate relationship existing between PCC and malware usage (B = 0.50, SE = 0.04, 8 = 0.57, p < .001), and PCC accounts 33 percent of variance in malware usage ($R^2 = 0.33$). This implies that someone who believes that there is a greater risk of cyber-crime is more prone to experience or get infected with malware. The fact that the statistical significance (F(1, 276) = 134.79, p <. 001) supports the notion that there is a possibility that the risks of malware can be mitigated by enhancing awareness about cyber-crime. With the increase in PCC, the chances of exposure to malware increases and this is where educating on cybersecurity becomes crucial to curb such threats. The outcomes of the case of online scams demonstrate a weak positive correlation (B = 0.18, SE = 0.03, 0.30, p < .001), which accounts to 9.2% of the variation ($R^2 = 0.09$). Even though the correlation is less than that of malware, it remains significant (F (1, 276) = 28.12, p <.001). This implies that people that have a greater understanding of cyber-crime are more likely to be deceived by scams on the internet, which means there is the need of raising awareness to ensure that such events are avoided. The result of the analysis of harassment shows that the relationship between the two is weak (B = -0.07, SE =0.02 0 = -0.18, p =0.003), and PCC is only capable of explaining 3.2 percent of the variance in harassment (R^2 =0.03). This outcome suggests that those who are more likely to see a greater extent of cyber-crime might have reduced chances of being harassed, possibly because they are more cautious in cyberspace. The model has been proved to be statistically significant (F (1, 276) = 8.99, p = 0.003), which explains the fact that cyber-crime awareness can be used to reduce online harassment. Regression of anti-virus software indicates that there is a moderate positive relationship (B = 0.36, SE = 0.04, 0.47 = 0.22), and PCC explains the 21.6 percent of variation in the use of anti-virus software ($R^2 = 0.22$). The statistical significance (F(1, 276) = 76.25, p <.001) indicates that people with greater PCC tend to use anti-virus software as a protective measure. This observation explains why there is a need to create awareness about cyber threats to instill proactive measures like use of anti-virus programs. The analysis is helpful in understanding how perception of cyber-crime can affect such behavioral patterns as malware use, Internet frauds, harassment, and anti-virus software adoption. Even though the intensity of such relationships may differ, the general results insist on continuous work to inform people about cyber-crime, which would result in more protective behavior and it may cause the decreasing effects of cyber threats.

FINDINGS AND DISCUSSION

The findings of the study regarding the cyber-crime awareness among prospective teachers of public sector universities of Punjab, Pakistan give good idea about the awareness of the prospective teachers towards cyber threats and about the utilization of the safety measures in it. Table 2 indicates the internal consistency of the scales used to measure each of the constructs: perception of cyber-crime (α = .712), malwares (α = .735), phishing (α = .807), online scams (α = .723), harassment (α = .775), frauds involving electronic funds transfers/credit cards (α = .578), password usage (α = .791), anti-virus software (α = .755) and social engineering (α = .858). The results of the reliability analysis showed that the items measuring these constructs are consistent, and appropriate for analysis (Alhanatleh, et al., 2024).

Prospective teachers' awareness of cyber-crime and cyber threats were of moderate degree as reflected in the descriptive statistics and bivariate correlations. Additionally, the means of phishing (M = 26.70, SD = 5.14) and the scores related to the usage of passwords (M = 34.68, SD = 6.99) were higher, which means

that they were more focused on the areas of phishing and password use, while the scores for harassment (M = 10.55, SD = 4.73) and fraud on credit card (M = 14.10, SD = 4.33) were lower, indicating less attention paid to harassment and fraud on credit cards in regard to cyber security (Bognár & Bottyán, 2024). Significant positive correlations were observed between perception of cyber-crime (PCC) and malware (MW, $r = .576$, $p < .001$), online scams (OS, $r = .295$, $p < .001$), harassment (HS, $r = .296$, $p < .001$), and anti-virus software usage (AVS, $r = .283$, $p < .001$). This suggests that the more aware people are of cyber-crime the more likely they are to be engaged in protective behaviors, consistent with earlier studies which showed the relationship between awareness and security behaviours (Jin et al., 2025). Likewise, there were strong positive correlations with social engineering (SE) and phishing (PS, $r = .496$, $p < .001$), harassment (HS, $r = .498$, $p < .001$), and credit card fraud (FC, $r = .500$, $p < .001$), indicating that those who are better informed on cyber threats are likely to be more aware of manipulative online activities that pose risks to their personal information (Balakrishnan et al., 2025).

Additionally, regression analysis reveals the predictive ability of cyber-crime perception on safety behaviours. PCC was a strong predictor of the use of malware ($B = 0.50$, $\beta = 0.57$, $p < .001$, $R^2 = 0.33$), suggesting that the greater the perception of cyber threats the more likely a person is to experience or encounter malware (Alhanatleh et al., 2024). The online scam awareness also showed a positive but less strong effect ($B = 0.18$, $\beta = 0.30$, $p < .001$, $R^2 = 0.09$) indicating that awareness partially predicts vulnerability to internet fraud (Bognár & Bottyán, 2024). PCC and harassment had a negative and weak correlation ($B = –0.07$, $\beta = –0.18$, $p < .01$, $R^2 = 0.03$), suggesting that as awareness increases, the risk of being harassed online decreases. Lastly, PCC significantly predicted the use of anti-virus software ($B = 0.36$, $\beta = 0.47$, $p < .001$, $R^2 = 0.22$), highlighting the importance of awareness in promoting proactive protective behaviours (Balakrishnan et al., 2025). The regression results support the earlier findings that the informed attitude is correlated with taking protective actions and decreasing exposure to cyber threats (Alhanatleh et al., 2024; Bognár & Bottyán, 2024; Jin et al., 2025).

Results also indicate that there is a lack of protective behaviors and reporting procedures in prospective teachers. Use of anti-virus software is positively correlated to cyber-crime perception, but reporting online incidents and resisting social engineering attacks are still relatively untouched fields (Jaishankar & Halder, 2011). This is consistent with the literature highlighting the importance of structured education and awareness-raising campaigns for improving students and future teachers' cyber security awareness (Balakrishnan et al., 2025).

Perceived cyber-crime is related to phishing, online scams, harassment and fraud, highlighting the importance of educating prospective teachers about these threats. It is essential to raise awareness and provide educational interventions to identify and minimise these risks, particularly as students are avid social media and online platform users (Jin et al., 2025). Improved awareness of proper password use, anti-virus and social engineering defences can enable future teachers to ensure their own security and help their students learn in a secure online environment (Bognár & Bottyán, 2024).

Finally, perceived cyber-crime is an important factor for prospective teachers' protective behaviors. The moderate awareness levels and positive correlations with safety measures highlight the importance of interventions and cyber education programs. To ensure that future teachers are able to use the digital world in a safe and responsible manner, educational institutes in Pakistan must implement comprehensive cyber-crime awareness and prevention strategies that include proper usage of reporting mechanisms and security tools (Alhanatleh et al., 2024; Jaishankar & Halder, 2011; Balakrishnan et al., 2025).

CONCLUSION

According to the findings of this research, the potential teachers do not have much knowledge regarding

cyber-crime. This implies that most of the new teachers do not understand the different types of cyber-crime that they may be exposed to. So, as much as technology has been applied in the higher education world, it has been evident that there is an urgent training requirement to de-sensitize students on matters of cyber-security so that they do not fall prey to cyber-crime. According to the findings, future educators are susceptible to cyber-crimes, but they are not aware of the latest threats (phishing, credit card fraud, online frauds, illicit downloading, industrial espionage, exploitation of children, cyber acts of terror and selling malicious programs). These dangers are common on digital platforms, such as chat rooms, emails and social media. This is why it is necessary to increase thei r awareness of such threats and provide the knowledge needed to defend themselves when utilizing the new communication networks and portable devices.

RECOMMENDATIONS

1. Higher education institutions may consider teaching cyberspace security to raise students' awareness and reduce cyber-crime victimization.

2. Promoting cyber-crime awareness programs among students, especially aspiring teachers, may enhance their understanding of cyber-crimes and self-protection.

3. NR3C may organize workshops and conferences in higher education institutions to educate students about cyber-crimes and reporting mechanisms.

4. Universities may launch online portals to raise awareness about cyber-crimes and provide a platform for reporting incidents.

REFERENCES

Adeshola, I., & Oluwajana, D. (2024). Assessing cybersecurity awareness among university students: implications for educational interventions. *Journal of Computers in Education*, *12*(4), 1283. https://doi.org/10.1007/s40692-024-00346-7

Adey, N. H., Mee, S. K. S., & Ading, C. E. (2025). Exploring Teachers' Awareness and Preparedness for Cyberbullying in Malaysia: A Systematic Review (2018-2024) [Review of *Exploring Teachers' Awareness and Preparedness for Cyberbullying in Malaysia: A Systematic Review (2018-2024)*]. *International Journal of Research and Innovation in Social Science*, 3895. https://doi.org/10.47772/ijriss.2025.9010304

Akter, M., & Wiśniewski, P. (2025). Moving Beyond Parental Control toward Community-based Approaches to Adolescent Online Safety. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2503.22995

Alhanatleh, H., Khaddam, A., Abu-Dabaseh, F., Alghizzawi, M., & Alzghoul, A. (2024). Enhancing the public value of mobile fintech services through cybersecurity awareness antecedents: A novel framework in Jordan. *Investment Management and Financial Innovations*, *21*(1), 417. https://doi.org/10.21511/imfi.21(1).2024.32

AlQarni, A. (2025). The relationship between cybersecurity awareness and data protection behaviors among Saudi secondary school students: the mediating role of cyber threat perception and the moderating role of internet usage duration. *Humanities and Social Sciences Communications*, *12*(1). https://doi.org/10.1057/s41599-025-06122-x

Andria, A., Laksono, R. D., Sussolaikah, K., M-Dawam, S. R., Din, M. M., & Mansor, S. (2025). BRIDGING THE GAPS: EVALUATING CYBERSECURITY AWARENESS AND PRACTICES FOR ENHANCED DIGITAL SECURITY. *Journal of Information System and Technology Management*, *10*(38), 202. https://doi.org/10.35631/jistm.1038013

Balakrishnan, V., Ahhmed, U., & Basheer, F. (2025). Personal, environmental and behavioral predictors associated with online fraud victimization among adults. *PLoS ONE*, *20*(1). https://doi.org/10.1371/journal.pone.0317232

Bhatt, R. K., & Shah, K. (2025). A Detailed Exploration of the Security Issues in Educational Applications. In *Lecture notes in networks and systems* (p. 145). Springer International Publishing. https://doi.org/10.1007/978-981-97-8605-3_14

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

Childers, G., Pinheiro, W. A., Daramola, O. O., Linsky, C. L., Payne, B., Byers, J., & Baker, D. N. (2025). Exploring K-12 Teachers' Definitions and Perspectives of Cybersecurity. *Journal of Cybersecurity Education Research and Practice*, *2025*(1). https://doi.org/10.62915/2472-2707.1218

Dewi, N. K. R. K. (2025). ANALISIS KRITIS TEORI KONTROL SOSIAL DAN APLIKASINYA DALAM PENCEGAHAN KEJAHATAN KOMUNITAS. *Jurnal Aktual Justice*, *10*(1), 79. https://doi.org/10.70358/aktualjustice.v10i1.1504

Hockly, N. (2023). Artificial Intelligence in English Language Teaching: The Good, the Bad and the Ugly. *RELC Journal*, *54*(2), 445. https://doi.org/10.1177/00336882231168504

Ibrahim, N., & Rajalakshmi, N. R. (2025). Examining the Influence of Advanced Persistent Threats on Higher Education Institutions and Investigating Appropriate Cybersecurity Strategies. *U Porto Journal of Engineering*, *11*(2), 96. https://doi.org/10.24840/2183-6493_0011-002_002671

Jin, S., Baek, H., Lee, U., & Kim, H. (2025). *I Was Told to Install the Antivirus App, but I'm Not Sure I Need It: Understanding Smartphone Antivirus Software Adoption and User Perceptions*. 1. https://doi.org/10.1145/3706598.3713452

Karayol, M., Murathan, T., Erdoğan, R., Akarsu, M., Baş, M., & Norman, G. (2025). Investigating the relationship between digital citizenship levels and cyberbullying attitudes of university students. *Frontiers in Psychology*, *16*. https://doi.org/10.3389/fpsyg.2025.1664397

Khan, A. R. A. (2025). Cyber Crime in Pakistan: Trends, Challenges, and Legal Responses. *Advance Social Science Archive Journal*, *4*(1), 1358. https://doi.org/10.55966/assaj.2025.4.1.080

Kont, K. (2025). Cyber Threat Risks in Higher Education Institutions: an Example of the Estonian Academy of Security Sciences. *Baltic Journal of Modern Computing*, *13*(2). https://doi.org/10.22364/bjmc.2025.13.2.11

Lamond, M., Prior, S., Renaud, K., & Wood, L. A. (2025). Teachers' perspectives and practice of cybersecurity education in primary schools. *Discover Education*, *4*(1). https://doi.org/10.1007/s44217-025-00471-0

Lazarov, W., Schafeitel-Tähtinen, T., Squillace, J., Martinásek, Z., Coufalíková, A., Helenius, M., Gallus, P., & Fujdiak, R. (2025). Lessons Learned from Using Cyber Range to Teach Cybersecurity at Different Levels of Education. *Technology Knowledge and Learning*. https://doi.org/10.1007/s10758-025-09840-y

Long, S. (2025). Systematic Review of Elementary Cybersecurity Education: Curriculum, Pedagogy, and Barriers. *Journal of Cybersecurity Education Research and Practice*, *2025*(1). https://doi.org/10.62915/2472-2707.1265

Maria, M., Makhdum, F. N., Sandhu, Ms. R. K., Khan, S., & Younas, A. (2025). Smart Learning in Pakistani Universities: A Mixed-Methods Study of Progress, Challenges, and Future Directions. *Research Journal for Social Affairs*, *3*(5), 173. https://doi.org/10.71317/rjsa.003.05.0316

Masudi, N. M. Dr. J. A. (2023). CYBER SECURITY AND DATA PRIVACY LAW IN PAKISTAN: PROTECTING INFORMATION AND PRIVACY IN THE DIGITAL AGE. *Pakistan Journal of International Affairs*, *6*(3). https://doi.org/10.52337/pjia.v6i3.906

Mui, J. Y., Eversole, B. A. W., & Crowder, C. L. (2025). *In-Person and Remote Employees and Information Security Policy Compliance* (p. 91). https://doi.org/10.1007/978-3-031-92548-1_6

Nadiba, Z. (2025). Empowering the Next Generation: A Research Proposal for Cybersecurity Education in the School Curriculum. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5066660

Olayinka, T. A. (2025). Discerning cybers' threats in an era of digitally connected classrooms: lessons for the Nigerian higher education system and society. *Discover Computing*, *28*(1). https://doi.org/10.1007/s10791-025-09564-8

Safdar, S., Mahmood, A., Hameed, B., & Muhammad, Y. (2025). Between Tradition and Technology: A Phenomenological Exploration of Digital Citizenship Knowledge Gaps Among Female Pre-service Teachers in Pakistan. ˜ *The œcritical Review of Social Sciences Studies*, *3*(2), 445. https://doi.org/10.59075/7j1awy31

Salam, M., Bakar, K. A. A., & Aman, A. H. M. (2025). Building Cyber-Resilient Universities: A Tailored Maturity Model for Strengthening Cybersecurity in Higher Education. *International Journal of Advanced Computer Science and Applications*, *16*(5). https://doi.org/10.14569/ijacsa.2025.0160510

Shari, M. B. K. B. (2025). Role of Restorative Justice in Strengthening Social Ties and Reducing E-Crime using Social Bond Theory (SBT) and Re-integrative Shaming Theory (RST). *Journal of Ecohumanism*, *4*(2). https://doi.org/10.62754/joe.v4i2.6504