Bahria Journal of Professional Psychology, July 2026, Vol. 25, No. 1, 67–81

Cybercrime Awareness, Cybersecurity Practices, and Perceived Self-Efficacy Among Young Adults

* Khadija Tul Uzma[1], Afifa Anjum[1], and Muhammad Abdullah[2]

[1]Institute of Applied Psychology, University of the Punjab, Lahore, Pakistan

[2]Department of Computer Science, University of Engineering and Technology (UET), Lahore, Pakistan

The present study focused on awareness, victimisation, cybersecurity practices, reporting awareness and perceived self-efficacy of cybercrime protection amongst the young adults of Pakistan. Additionally, the study investigated how experiences with cybercrime are related to protective practices and perceived self-efficacy. Cross-sectional correlational research was carried out on a convenience sample of 120 university students. The Demographic Information Form, the Cybercrime Awareness and Protection Questionnaire (CAPQ) and the modified General Self-Efficacy Scale (Jerusalem & Schwarzer, 1981) were used for data collection. Data analysis methods were descriptive statistics, Pearson correlation, independent-samples t-tests and analysis of variance (ANOVA). Results revealed moderate level of awareness of common cybercrime offences and perceived self-efficacy but poor knowledge of reporting mechanisms and the Prevention of Electronic Crimes Act (PECA), 2016. There were no significant relationships between cybercrime experiences and protective practices and perceived self-efficacy, though the relationship was positive. The results reinforce the need for blended training and knowledge on cybersecurity awareness and legal knowledge.

Keywords. Cybercrime awareness, Cybercrime victimisation, Cybersecurity practices, Perceived self-efficacy, PECA 2016, Young adults

*Correspondence concerning this article should be addressed to Khadija tul Uzma, Institute of Applied Psychology. University of the Punjab, Lahore, Pakistan. Email: ktuzme@gmail.com

Digital technologies have led to an unprecedented transformation of human communication, education, employment, and information about the world. By the beginning of 2026, the number of people using the internet is over 6.12 billion, or 73.8% of the world's population, which is a five-fold increase from the amount using the Internet in 2010 (DataReportal, 2026). The internet has become an integral component of daily existence, even for young adults who use the web extensively for learning, socializing, conducting finances and watching entertaining presentations. The same metamorphosis is also being witnessed in Pakistan with 207 million telecom subscribers and 150 million broadband connections recorded at the end of 2025, making broadband penetration stand at 64.2% (Annual Report of Pakistan Telecommunication Authority, 2024-25; Economic Survey of Pakistan, 2025-26). While these technological advances have created numerous opportunities, they have also increased individuals' exposure to cyber threats and online criminal activities.

Cybercrime is defined as any crime while using a computer, digital device or network of computers via the internet or other electronic means, which is intended to affect the integrity of information systems, financial assets, personal information, or privacy. It covers violations of privacy involving the breach of information, electronic fraud, identity theft, cyberstalking, malicious software, spoofing, phishing, electronic forgery and cyber terrorism. These offences may lead to financial and property damages, psychological anguish, harm to reputation or invasion of privacy. As cybercrime becomes ever more complex, it is important to be aware of the

vulnerabilities of technology but also of the human factors and how these will affect individuals' ability to identify and react to online threats.

In the last ten years, the situation of cybercrime has grown dramatically. By 2025, global losses from cybercrime are estimated to have reached as high as $10.5 trillion, making it the third largest economy in the world, trailing the United States and China (Cybersecurity Ventures, 2025). The FBI's Internet Crime Complaint Centre (IC3) reported receiving more than a million Internet crime complaints in 2025, resulting in losses of nearly $21 billion compared with a 26% increase in reported Internet crime losses from 2024 (FBI, 2026). Similarly, there has been a rise of cyber threats in Pakistan. Since 2020, the FIA has received more than 649,000 complaints of cybercrime, but only 222 convictions have been obtained, according to The News International (2025). The problem of digital fraud is enormous, accounting for an estimated 2.5% of Pakistan's GDP, which costs the nation an estimated “$9.3 billion” (Global Anti-Scam Alliance & Feedzai, 2025) every year.

In this context, two psychological constructs are relevant to the understanding of individual vulnerability and individual resiliency against cybercrime: awareness and perceived self-efficacy. Cybercrime awareness is the extent to which one is aware of cybercrime types, definitions, legislation and consequences. A pattern has been consistently found in the literature that awareness has significant impact on protective behaviour – that is, people who know what constitutes a cybercrime and what legal enforcement options are available are much more likely to take proactive steps to protect themselves (Goel, 2014; Muniandy et al., 2017; Tonkolu, 2019).

Perceived self-efficacy, as developed by Bandura (1997, 1994) and expanded by Maddux (2009), is a person's confidence in their ability to perform behaviours necessary to obtain a desired outcome in a specific situation. For cybersecurity, self-efficacy is the extent to which people feel they are capable of handling, solving, and defending themselves against cyber threats. Rhee et al. (2009) have shown that cybersecurity self-efficacy positively relates to the use of security software, the application of patches, and other evidence-based self-protective behaviour s. Storing awareness training also improves self-efficacy for cyber security which leads to security conscious behaviour, as previously found by Tonkolu (2019).

Previous studies mostly have focused on either cybercrime awareness, cyber safety behaviour, digital literacy, or cyber victimisation. There are relatively few studies that have explored these factors in a combined study, let alone within a Pakistani context. Also, the majority of the existing measures focus on only a single aspect of cyber security and do not give sufficient data on people's experiences with cybercrime, protective measures, awareness of reporting systems, or knowledge on cybercrime laws. This restricts the depth of understanding about how young adults view and react to cyber risks in everyday life.

To fill this gap, the present study used the Cybercrime Awareness and Protection Questionnaire (CAPQ), which is a multidimensional questionnaire developed by researchers specifically for the Pakistani context. The CAPQ is a joint development of psychology researchers and an expert in information technology that examines several aspects relevant to cybercrime, such as knowledge of cyber offences, victimisation experiences, online protective behaviour, awareness of the reporting options and understanding of the Prevention of Electronic Crimes Act (PECA), 2016. The study's findings and analysis of these dimensions in addition to perceived self-efficacy, offer a more comprehensive picture of cybercrime awareness, cybercrime-related experiences, as well as protective practices within the context of young adults.

These issues have significant practical repercussions for psychological research, educating about cyber security, and public policy. This information can help develop educational interventions, awareness campaigns, and institution policies for promoting online safe behaviours among youth in Pakistan, by identifying strengths and gaps in awareness, online protective practices and confidence in online threat management.

The current study is based on Bandura's (1986, 1994) Social Cognitive Theory, which suggests that human behaviours are influenced by the interaction between personal cognitive factors, behavioural patterns and environment. In this approach, belief in one's ability to plan and perform the actions needed to plan ahead to meet challenges effectively is recognized as one of the major cognitive factors that influence action. Mastery experiences, vicarious experiences, verbal persuasion and physiological states are the four main sources of self-efficacy.

Social Cognitive Theory proposes that knowledge cannot be a determinant in changing behaviour. People also need to see a chance for them to be able to do the behaviour successfully. So, the perceived self-efficacy was thought to be a relevant psychological variable to explain cybersecurity-related behaviours in young adults.

In the field of cybersecurity, people who have more self-efficacy are more likely to engage in protective online actions, react to cyber threats, and continue to take cybersecurity measures. Awareness training is a training that provides knowledge to identify the cyberthreats and assists building self-efficacy in applying protective online behaviours (Rhee et al., 2009; Tonkolu, 2019). Thus, self-efficacy was deemed to be a significant psychological variable to be explored in online protection among young adults.

Research in Pakistan has so far looked at cybercrime awareness, digital literacy or online behaviour separately despite the escalating frequency of cybercrime in Pakistan. Few studies have considered the concept of cybercrime awareness, cybercrime victimisation experiences, cybercrime protections, cybercrime reporting awareness and cybercrime perceived self-efficacy in a single model. In addition, no multidimensional instrument specifically developed for Pakistani context was found. While previously, researchers have reported the spread of cybercrime in Pakistan (Munir & Shabir, 2018; Soomro & Hussain, 2019; Khan et al., 2018), the awareness of the legal framework regulating these kinds of crimes is alarmingly low (Zia ul Islam et al., 2019).

Knowing the relationship between cybercrime-related experiences and protective practices and perceived self-efficacy provides insight into whether education about cybercrime awareness will have a downstream effect in terms of increased self-efficacy and actual protective practices in the behaviours of young adults in Pakistan. This study's objective is to fill these gaps by utilizing Cybercrime Awareness and Protection Questionnaire (CAPQ) to assess the awareness about cybercrime, cybercrime experiences, protective practices and perceived self-efficacy among young Pakistanis.

Objectives

The present study was designed to achieve the following objectives:

1. To assess the level of cybercrime awareness among young adults in Pakistan.
2. To examine cybercrime victimisation experiences and cybersecurity practices among young adults in Pakistan.
3. To examine perceived self-efficacy for protection against cybercrime among young adults in Pakistan.
4. To examine the relationship between cybercrime-related experiences and protective practices and perceived self-efficacy for protection against cybercrime among young adults in Pakistan.

Hypothesis

1. There is likely to be a significant positive relationship between cybercrime-related experiences and protective practices and perceived self-efficacy for protection against cybercrime among young adults.

Method

Research Design

The present study employed a cross-sectional correlational research design. A cross-sectional design was considered appropriate because data were collected from participants at a single point in time. The correlational approach was used to examine the relationship between cybercrime-related experiences and protective practices and perceived self-efficacy among young adults. No variables were manipulated, and no intervention was introduced during the study.

Sample

The study included 120 young adults (37 males, 30.8%; 83 females, 69.2%) enrolled in universities and colleges in Lahore, Pakistan. Participants were recruited using a convenience sampling technique. Data were collected through an online survey administered via Google Forms. The survey link was distributed through university WhatsApp groups, class WhatsApp groups, and personal contacts. Participation was voluntary.

An a priori power analysis was conducted using G*Power version 3.1.9.7 to estimate the minimum sample size required for the study. The analysis indicated that a minimum sample of 84 participants was required. Therefore, the final sample of 120 participants exceeded the required sample size and was considered adequate for the planned analyses.

Participants ranged in age from 18 to 28 years ($M = 21.76$, $SD = 2.25$). Enrolment in college or university, age range and being active internet users were the requirements to participate. As a criterion of participation, active use of the internet was linked to the participants' answers to the questions of how frequent they use the internet, what is their mean time spent on the internet per day and what kind of devices they use to connect to the internet.

Regarding educational level, 8 (6.7%) participants were enrolled in FA/FSc, 14 (11.7%) in BA/BSc, 50 (41.7%) in BS programmes, 41 (34.2%) in MSc programmes, and 7 (5.8%) in MS/MPhil programmes. Demographic information was gathered as a demographic variable to describe the socioeconomic characteristics of the sample and to examine demographic differences on the study variables, namely monthly family income.

Assessment Measures

Demographic Information Form

Participants' age, gender, level of education and monthly family earnings were all recorded on a demographic information form. Data on use of the internet also was gathered such as frequency of internet use, average time spent online per day, internet accessing devices, purpose of using the internet, number of e-mail accounts, and social media platforms used. These were also employed to validate the subjects as active Internet users.

Cybercrime Awareness and Protection Questionnaire (CAPQ)

The Cybercrime Awareness and Protection Questionnaire (CAPQ) was used to assess cybersecurity related information. The questionnaire was created cooperatively between the psychologists and an information technology expert. This allowed for both the psychological and

technical sides of cybersecurity to be well represented. The content on cybersecurity and technical terminology was created by the first and second authors, both of whom have backgrounds in psychology, and interaction with the Prevention of Electronic Crimes Act (PECA), 2016 was done under the supervision of the third author. The third author is a professional in information technology, with long experience in information security and computer forensics and network administration. This attempt of interdisciplinarity was taken to facilitate the relevance of the questionnaire to the technological context and to allow for conceptual clarity in psychological research. The questionnaire was checked by experts in psychology and information technology to ensure content validity and items were relevant, clear and representative of the constructs of the study.

CAPQ was a set of seven sections. The first section was a measure of participants' knowledge of offences that constitute cybercrime under PECA (2016). The second part measured the experiences of cybercrime victimisation in the context of these crimes. The third section discussed why participants indulged in online actions that they subsequently regretted. Online self-security practices with respect to the protection of personal information and digital privacy are covered in section 4. The fifth section focused on where participants got advice regarding internet safety. The sixth section relates to the awareness of cybercrime reporting agencies, reporting process in PECA (2016) and legal provisions. Each of these six sections contained dichotomous (Yes/No) items and categorical and multiple response items. The frequency and percentage analysis were used to analyse the data obtained from these sections.

The last part (No. 7) was the psychometric part of the questionnaire. It was comprised of 7 items measuring cybercrime-related experiences and protective practices that used the Likert scale format. The answers were answered on a five-point scoring system from 1 (Never) to 5 (Not Cared About It). Responses were totalled across the seven items to get a composite score. This score was utilized in reliability analysis and for all other inferential analysis such as, Pearson correlation, independent samples t-test, and one-way analysis of variance (ANOVA). The internal consistency of the scale was satisfactory (Cronbach's $\alpha = .69$).

Modified General Self-Efficacy Scale

Perceived self-efficacy for protection against cybercrime was measured using a modified version of the General Self-Efficacy Scale developed by Jerusalem and Schwarzer (1981). Permission to adapt the scale was obtained from the original authors before data collection. Eight of the ten items were adapted to reflect cybersecurity situations, whereas two items remained unchanged. Responses were recorded on a four-point Likert scale ranging from 1 (Not at All True) to 4 (Exactly True), with higher scores indicating greater perceived self-efficacy for protection against cybercrime. In the present study, the modified scale demonstrated good internal consistency (Cronbach's $\alpha = .85$).

Procedure

Ethical approval for the study was obtained from the Institute of Applied Psychology, University of the Punjab, Lahore. Permission to adapt the General Self-Efficacy Scale was obtained from the original authors prior data collection.

Data were collected online using Google Forms. The survey link was distributed through university WhatsApp groups, class WhatsApp groups, and personal contacts. Participants were informed about the purpose of the study, confidentiality of their responses, voluntary participation, and their right to withdraw from the study at any stage without penalty. Informed consent was obtained electronically before participants completed the questionnaires.

Data Analysis

Data were analysed using IBM SPSS Statistics Version 21. Prior to analysis, the dataset was screened for missing values, outliers, and data entry errors. No substantial missing data or data entry errors were identified. Descriptive statistics, including frequencies, percentages, means, and standard deviations, were computed to summarise participant characteristics and the descriptive components of the CAPQ.

Internal consistency reliability was assessed using Cronbach's alpha for the psychometric component of the CAPQ and the Modified General Self-Efficacy Scale. Pearson product-moment correlation analysis was conducted to examine the relationship between cybercrime-related experiences and protective practices, perceived self-efficacy, and age. Independent-samples *t*-tests were used to examine gender differences, whereas one-way analysis of variance (ANOVA) was conducted to examine differences across educational level and monthly family income. Statistical significance was set at $p < .05$.

Ethical Considerations

Research procedures employed were conducted ethically as expected in the field of psychological research. Informed consent was taken electronically prior to participation. Participants were promised confidentiality and anonymity of their response. All contacts with participants were voluntary, and the respondents were provided with information that they were free to withdraw at any time without any consequences. Only for research purposes data were used.

Results

Descriptive Findings

Cybercrime Awareness

The initial section of the CAPQ focused on participants' knowledge of 14 cybercrime offences outlined in the Prevention of Electronic Crimes Act (PECA), 2016. The average percentage of awareness for the different offence categories was between 60% and 70% which represents moderate awareness among the participants. The number of offences and their percentages are displayed in Table 1.

Table 1

Descriptive Statistics of Awareness About Cybercrime Types (N = 120)

Variables	*f*	*%*
Cyberstalking	84	70
Offense against dignity/ modesty of a natural person	82	68
Electronic fraud	80	67
Unauthorized use of identity information	80	67
Unauthorized access/ copying/ transmission/or interference of data	79	66
Electronic forgery	79	66
Making, obtaining, or supplying device for use in offense	79	66
Spoofing	79	66
Cyber terrorism	78	65
Malicious code	78	65
Glorification of an offense	76	63
Child pornography	74	62
Spamming	74	62
Unauthorized issuance of SIM card	72	60

Note. f=Frequency, %=Percentage.

Participants were asked whether they had personally experienced any of the cybercrime offences listed in the questionnaire. Electronic fraud was the most frequently reported form of victimisation, followed by unauthorised access to data, cyber terrorism, unauthorised use of identity information, and spamming. The detailed findings are presented in Table 2.

Table 2

Descriptive Statistics of Cybercrime Victimisation Experiences (N = 120)

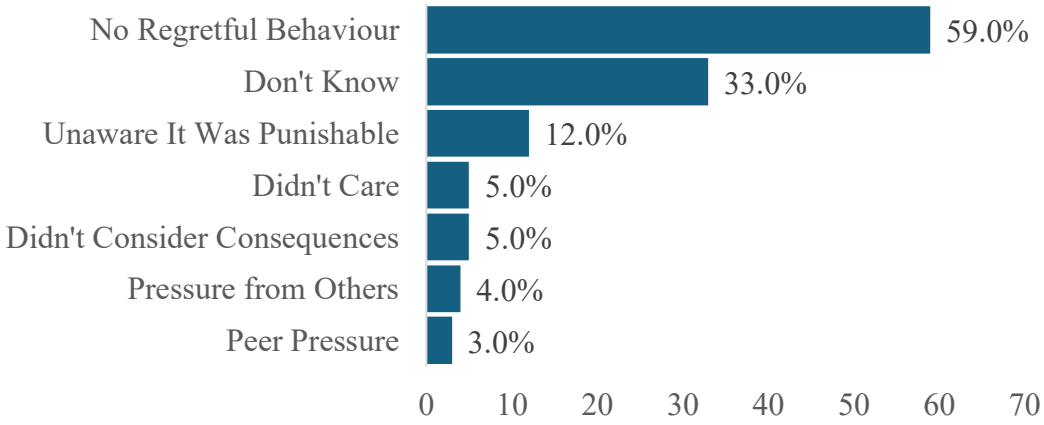
Variables	*f*	*%*
Electronic fraud	33	28
Unauthorized access/ copying/ transmission or interference of data	29	24
Cyber terrorism	29	24
Unauthorized use of identity information	29	24
Spamming	29	24
Unauthorized issuance of SIM card	26	22
Glorification of an offense	23	19
Malicious code	23	19
Offense against dignity/ modesty of a natural person	22	18
Cyberstalking	22	18
Spoofing	21	18
Making, obtaining, or supplying device for use in offense	20	17
Electronic forgery	19	16
Child pornography	13	11

Note. f=Frequency, %=Percentage.

Participants who indicated that they had engaged in online activities they later regretted were asked to identify the reasons for those behaviours. Most participants reported that they had not engaged in any online behaviour they regretted, whereas others reported lack of awareness or failure to consider the consequences of their actions. The detailed findings are shown in figure 1.

Figure 1

Reasons for Regretful Online Behaviour Among Young Adults (N = 120)



Online Self-Security Practices

The CAPQ was also designed to evaluate the protective measures taken by participants to keep their online privacy and security. The results show that the most frequently mentioned protective practices were changing passwords often, and not sharing passwords or using strong passwords. All results are detailed in Table 3.

Table 3

Descriptive Statistics of Self-Security Practices (N = 120)

Variables	*f*	*%*
Installed anti-virus software on personal device(s).	0	0.0
Changing password periodically.	64	53.3
Never shared the password with any family member, friend, or colleague.	58	48.3
Choosing hard-to-guess/ break passwords.	50	41.7
Avoided sharing of unnecessary personal information. (home address, personal cell no, etc.)	49	40.8
Avoided friendship requests/ chat requests from unknown people	49	40.8
Locking the device when leaving it unattended (laptop/ PC/ mobile etc.)	48	40
Avoided email attachments from unknown sources.	41	34.2
Never shared personal device(s) (Personal laptop, tab, cell phone, etc.)	39	32.5
Deleted no more required/ hacked online account(s). (Facebook page, hacked email account, etc.)	19	15.8
Any Other action was taken by yourself to secure you in cyberspace.	14	11.7
Cared nothing special.	7	5.8

Note. f=Frequency, %=Percentage.

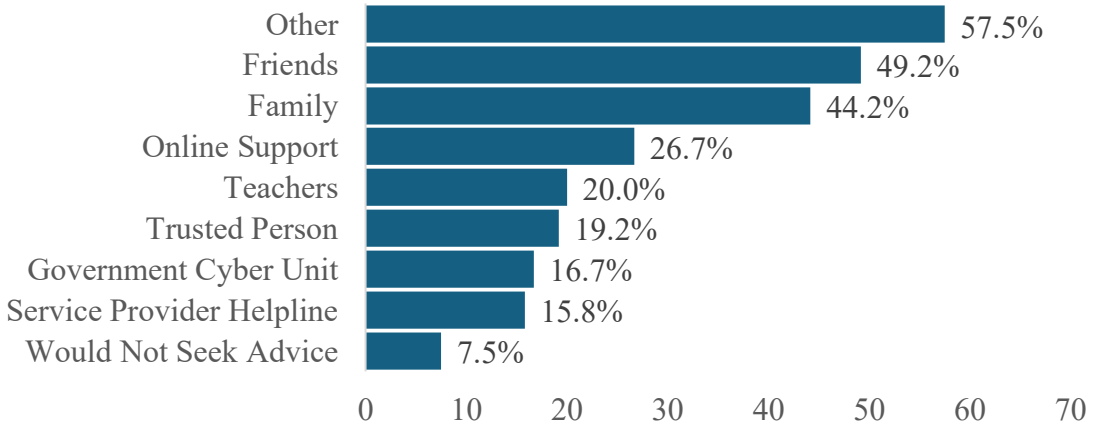
Specifically, none of the participants reported having anti-virus software on their personal devices, representing a possible lack of cybersecurity practices, as well as moderate indicators of cybercrime awareness.

Sources of Advice for Online Safety

The CAPQ also gauged participants' sources for getting useful information about safety online. Advice was most commonly reported to come from friends, parents and family members. The detailed results are summarized in figure 2.

Figure 2

Sources of Advice for Online Safety Among Young Adults (N = 120)



Note. Percentages represent participants selecting each source of advice. Multiple responses were permitted for this figure only.

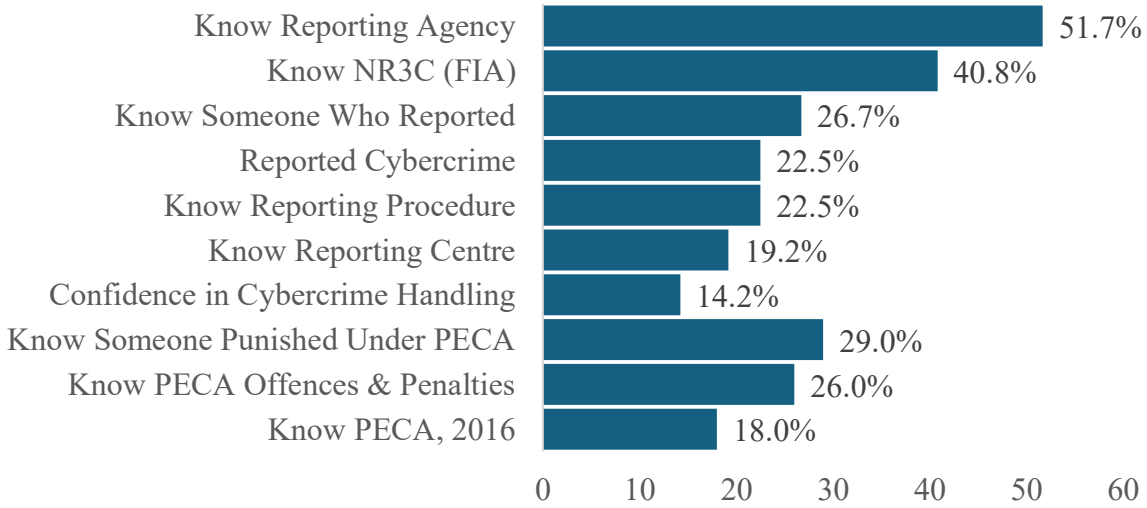
Awareness of Cybercrime Reporting Mechanisms and PECA 2016

The final descriptive section of the CAPQ examined participants' awareness of cybercrime reporting mechanisms, relevant government agencies, and the legal provisions of the Prevention

of Electronic Crimes Act (PECA), 2016. Overall, awareness of reporting agencies, reporting procedures, and cybercrime legislation was comparatively low. Although approximately half of the participants were aware that cybercrimes could be reported to a government agency, fewer participants were familiar with reporting procedures, organisational reporting centres, or the provisions of PECA (2016). The detailed findings are presented in figure 3.

Figure 3

Awareness of Cybercrime Reporting Mechanisms and the Prevention of Electronic Crimes Act (PECA), 2016 (N = 120)



Note. Percentages represent participants responding affirmatively ("Yes") to each awareness item. PECA = Prevention of Electronic Crimes Act; NR3C = National Response Centre for Cybercrime; FIA = Federal Investigation Agency.

Inferential Findings

Psychometric Properties of the Study Measures

Descriptive statistics and reliability analyses were conducted for the psychometric components of the study. The 7-item psychometric section of the CAPQ demonstrated acceptable internal consistency (Cronbach's α = .69), whereas the Modified General Self-Efficacy Scale demonstrated good internal consistency (Cronbach's α = .85). Participants obtained a mean score of 14.23 (SD = 4.89) on cybercrime-related experiences and protective practices and 27.78 (SD = 6.43) on perceived self-efficacy. The detailed findings are presented in Table 4.

Table 4

Descriptive Statistics and Reliability Coefficients for Study Variables (N = 120)

					Range	
Variables	*α*	*K*	*M*	*SD*	Potential	Actual
Cybercrime-Related Experiences and Protective Practices	.69	7	14.23	4.89	7-35	7-28
Self-efficacy	.85	10	27.78	6.43	10-40	11-29

Note. a=reliability coefficient, K=Number of Items, M=Mean, SD=Standard Deviation.

Pearson product-moment correlation analysis was conducted to examine the relationships among age, cybercrime-related experiences and protective practices, and perceived self-efficacy. Age showed a significant positive correlation with perceived self-efficacy, indicating that older participants reported slightly greater confidence in protecting themselves against cybercrime.

Although cybercrime-related experiences and protective practices was positively associated with perceived self-efficacy, the relationship was not statistically significant.

Table 5

Relationship Among Study Variables (N=120)

Variables	1	2	3
1. Age	-	.02	.18*
2. Cybercrime-Related Experiences & Protective Practices		-	.12
3. Self-efficacy			-

Note: *p<.05.

Independent samples t-tests indicated a significant gender difference in cybercrime-related experiences and protective practices, with male participants obtaining higher scores on cybercrime-related experiences and protective practices than female participants. However, no significant gender difference was observed in perceived self-efficacy. The detailed findings are presented in Table 6.

Table 6

Gender Differences in Study Variables (N = 120)

Variables	Male (n=37)		Female (n=83)				95% *CI*		
	M	*SD*	*M*	*SD*	*t*(118)	*p*	*LL*	*UL*	Cohen's d
Cybercrime-Related Experiences and Protective Practices	15.62	5.72	13.61	4.37	2.10	.03	.11	3.89	.38
Self-efficacy	27.76	5.70	27.78	6.76	-.02	.98	-2.5	2.50	.00

Note: CI=confidence interval, LL=lower limit, UL=upper limit, M=mean, SD=standard deviation.

Differences Across Educational Level and Monthly Family Income

One-way analyses of variance (ANOVA) were conducted to examine differences in cybercrime-related experiences and protective practices and perceived self-efficacy across educational levels and monthly family income groups. The analyses indicated no statistically significant differences in either study variable across the educational or income categories. These findings suggest that participants' levels of cybercrime-related experiences and protective practices and perceived self-efficacy were relatively similar regardless of their educational level or monthly family income.

Discussion

In the present study cybercrime awareness, cybercrime victimisation, online protective practice, awareness regarding cybercrime reporting mechanism, legislative provisions and perceived self-efficacy in cybercrime protection among the young adults in Pakistan were examined. It also explored the correlations between experiences of cybercrimes and protective practices and perceived self-efficacy. With the rapid change in cyber technologies, awareness of these factors has become ever more significant to both encouraging safer online behaviour, and designing and building effective cybersecurity education programs. The results of this study also add to the meagre psychological studies on cybercrime in Pakistan and offer implications for the education system and policy makers.

The descriptive results suggest that participants were very engaged with digital environments. Nearly all respondents said they were using the internet every day with their main source of internet access being their smartphone, and the WhatsApp communication platform

being used the most. The results concur with the earlier studies in Pakistan where it was found that the use of internet and social media is quite high among the university students (Bashir et al, 2008; Munir & Shabir, 2018). The same has been observed worldwide, as mobile technologies are the favoured method of digital access for youth-adults (Nguyen et al., 2020). Further evidence from more recent research also indicates that while university students are spending significant time online, high online spending time does not equal a superior cybersecurity knowledge and/or safer online behaviours (Alharbi & Tassaddiq, 2021). These findings taken together suggest that the digital world in which young adults navigate offers opportunities for positive communication and learning, but also exposes them to new cyber threats, so there is a need for an enhanced cybersecurity awareness and practice.

This further indicated that awareness was at a moderate level in relation to the fourteen Cybercrime offences evaluated in the Cybercrime Awareness and Protection Questionnaire (CAPQ). Participants had a general awareness of crimes involving commonly encountered electronic crimes such as electronic fraud, cyberstalking, unauthorised use of identity information crimes, but were less aware of the more specialised crimes involving electronic forgery, malicious code, spoofing, and using, making, obtaining, or supplying a device for use in an offence. The present results are in line with the previous research conducted by Senthilkumar and Easwaramoorthy (2017) and K. P & C (2017) which revealed that the cybercrime awareness among young internet users and university students is having moderate level. Likewise, in Pakistan a few studies have found that students may have had some experiences of common cyber threats due to personal experience or media coverage but do not know much about the cybercrime legislation or the formal reporting systems for cybercrime (Khan et al., 2018; Munir & Shabir, 2018). Such trends have been identified in recent research, which shows that generally university students are aware of some common cyber threats, but lack comparatively knowledge of legal frameworks, technical cyber threats, and university reporting protocols (Alharbi & Tassaddiq, 2021). The significant contrast in participants' awareness of cybercrime offences as compared to their awareness of the Prevention of Electronic Crimes Act (PECA) 2016 indicates that their knowledge about cybercrime is largely informal and experiential, rather than through formal cybersecurity training or legal literacy. The result highlights the importance of linking cybersecurity training to a sense of legal awareness, enabling young adults to identify the threats in cyberspace as well as be aware of their legal entitlements and reporting options, and where they can seek institutional assistance

Results also revealed that a significant number were victims of cybercrime in one or more of its forms, with electronic fraud and unauthorised access to personal information the most common types of cybercrime reported. Despite those experiences, participants also improvised a number of online protective practices such as having strong passwords, changing passwords frequently, not clicking on links they don't recognize or trust, and being careful not to share too much personal information. Low levels of consistency in the implementation of these protective practices, however, despite the participants' moderate awareness of common cybercrime offences. The result indicates that knowing doesn't always lead to consistent protective behaviour.

This finding aligns with Protection Motivation Theory, which suggests that people may just become aware of the danger, but not take protective action unless they think that they can do the appropriate security measures (Rhee et al., 2009). In the same way, Che Zainal et al. (2022) found that self-efficacy is a factor which influences the adoption decision of the protective behaviour following the acquisition of cybersecurity knowledge; this finding emphasizes the need to integrate knowledge sessions with practical training. The results indicate that cybersecurity

programs in schools should do more than educate about cyber security and offer hands-on learning experiences for cyber security skills through training, simulations, and/or guided practice.

The other significant outcome of the study was the low level of awareness about the reporting system for cybercrime, the Prevention of Electronic Crimes Act (PECA), 2016. While many participants were aware of the common cybercrime crimes, fewer knew about the appropriate reporting agencies, methods of reporting, and legal measures that exists in Pakistan. This is confirmed by the previous Pakistani studies which suggest that generally awareness of cybercrime is greater than the awareness of legal and institutional avenues for those who fall victim to cybercrime (Khan et al., 2018; Munir & Shabir, 2018). This difference indicates that among young adults, awareness of cyber threats may exist, but they may not know what to do if they find they have been targeted in cyberspace or are not sure how to seek help or report cyber incidents. Promoting better public understanding of reporting processes, institutional support services and laws on cybercrime should be regarded as a necessary element of national efforts in raising awareness about cybercrime. Improving the legal literacy in tandem with cyber security education can promote more reports of cybercrime and optimize people's trust on the existing support system.

The perceived self-efficacy in protection against cybercrime was moderate, suggesting that participants generally felt capable of handling online security issues. Surprisingly, however, cybercrime experiences and cybercrime protective practices had positive, though not statistically significant, relationships with perceived self-efficacy. This discovery points to the fact that awareness can be a facilitator of confidence, but experiences and protective behaviours might not be enough to build high levels of self-efficacy in cybersecurity. Bandura (1986, 1994) stated that, in addition to knowledge, self-efficacy is also influenced by mastery experiences, observational learning, social persuasion, and the past experiences in coping with difficult situations. When it comes to cybersecurity, people can know what's happening online, and also have the confidence to take the correct steps if they face a cyber incident in the real world. Self-efficacy positively influences information security behaviour, as shown in the study of college students in China by Han et al. (2025). These results reiterate the need to supplement awareness programmes with hands-on cyber training and practice of cyber skills to improve competence and confidence in dealing with online risks.

The results from the demographic analyses showed that for the male participants, there were more experiences and protection practices of cybercrime compared to the female participants, similar to recent findings by Ar-yuwat et al. (2025) on cybersecurity knowledge of university students in Thailand, where overall, male students demonstrated higher performances than their female counterparts for network security and malware detection, and in the areas of knowledge of encryption and key management. This distinction could be due to differing exposure to technology information, patterns of Internet use or opportunities for technology and cybersecurity education. Genders were not significantly different on perceived self-efficacy, however, scores on experiences with cybercrime and protective practices varied implying a similar level of confidence between male and female participants in their ability to handle cybersecurity issues. In addition, there was no significant association found between educational level and either cybercrime-related experiences and protective practices or perceived self-efficacy and between family income and either cybercrime-related experiences and protective practices or perceived self-efficacy.

These results suggest that demographic factors can be used to only a certain degree to explain differences in cybersecurity related behaviour. Certain other variables, like digital literacy, prior experiences with cybercrime, Internet use frequency and formal cybersecurity education,

could also have a more significant impact on individuals' sense of security and protective actions; their effects should be examined.

In overall context, the findings suggest that the cybercrime related experiences and protective practices were moderate among the young adults; they also reported that they had moderate self-efficacy and comparatively low levels of awareness of access points for reporting cybercrime and the provisions of the Prevention of Electronic Crimes Act (PECA), 2016. A correlation was found between cybercrime-related experiences and protective practices and perceived self-efficacy; however, this correlation was not statistically significant. Thus, the hypothesis under consideration was not accepted. The result shows that increasing awareness, without the ability to actually learn the right skills to deal with cyber threats, could be ineffective in boosting people's confidence in themselves to cope with cyber threats. Cybersecurity education and awareness programs should, therefore, combine awareness campaigns and hands-on training, cyber-literacy courses and chances for applied learning to cultivate both cybersecurity competence and confidence among young adults.

Conclusion

This research study seeks to shed light on the cybercrime awareness, cybercrime victimisation, online protective behaviours, knowledge about reporting procedures and perceived self-efficacy among young adults in Pakistan. The results showed that the participants had moderate knowledge about common cybercrime offences and had moderate self-efficacy but not very much knowledge related to cybercrime reporting and the laws related to the Prevention of Electronic Crimes Act (PECA), 2016. Experiences of cybercrime and protective practices were positively correlated with perceived self-efficacy but it was not statistically significant. The results indicate that mere awareness may not be enough to build the trust of individuals to be safe from cyber threats. Incorporating teaching of practical cyber security skills, digital literacy and legal awareness will help develop the skills of young adults to make safer choices while online and effectively respond to cyber threats.

Implications

The results have several implications for higher education institutions, policy makers and cybersecurity promotion organisations. The universities should have a built-in cyber security course in their curriculum and should be focused on practical activities, the safe use of the new technologies and the procedures for reporting cybercrime. Training programmes will not just be awareness-raising; they should also give students the chance to practise protective strategies in simulated real-life contexts by putting them into real-life scenarios and using practical exercises. Additionally, public awareness productions could be organized regarding the Prevention of Electronic Crimes Act (PECA), 2016, institutional support services and how to report. Better cooperation between educational institutions, the authorities, and security organizations could influence increased legal literacy, cybercrime reporting and promote safer online habits among young adults.

Limitations

The results of this study are subject to a few limitations. One is that the cross-sectional correlational design prevents causal inferences between the variables studied. On the other hand, participants were selected by using the convenience sampling technique from the universities and colleges of Lahore which restricts the generalisability of findings to the young adults of Lahore in the other regions of Pakistan. Third, self-report measures were used and this may have been affected by recall bias and social desirability. Last but not least, the psychometric properties of the Cybercrime Awareness and Protection Questionnaire (CAPQ) seemed to have good internal

consistency despite the lack of testing of the instrument's validity and psychometric properties on larger and more diverse samples.

References

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing, 5*(2), 23. https://doi.org/10.3390/bdcc5020023

Ar-yuwat, S., et al. (2025). Bridging the gap: How knowledge, attitudes, and practices shape cybersecurity awareness in Thai education. *Educational Process: International Journal, 16*, Article e2025236.

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Prentice-Hall.

Bandura, A. (1994). Self-efficacy. In V. S. Ramachaudran (Ed.), *Encyclopedia of human behaviour* (Vol. 4, pp. 71–81). Academic Press.

Bandura, A. (1997). *Self-efficacy: The exercise of control*. W. H. Freeman

Bashir, S., Mahmood, K., & Shafique, F. (2008). Internet use among university students: A survey in University of the Punjab, Lahore. *Pakistan Journal of Information Management and Libraries, 9*, 35–51. https://doi.org/10.47657/20089811

Che Zainal, N., Mohd Puad, M. H., & Mohd Sani, N. F. (2022). Moderating effect of self-efficacy in the relationship between knowledge, attitude and environment behaviour of cybersecurity awareness. *Asian Social Science, 18*(1), 55–63. 10.5539/ass.v18n1p55

Cybersecurity Ventures. (2025). *Global cybercrime damages report.*

DataReportal. (2026). *Digital 2026 global overview report. Meltwater & We Are Social.*

Economic Survey of Pakistan. (2026). *Economic survey of Pakistan 2025–26. Ministry of Finance, Government of Pakistan.*

Federal Bureau of Investigation. (2026). *2025 Internet Crime Report. Internet Crime Complaint Center.*

Global Anti-Scam Alliance, & Feedzai. (2025). *Global State of Scams Report 2025*.

Goel, U. (2014). Awareness among B.Ed. teacher training towards cyber-crime: A study. *Learning Community-An International Journal of Educational and Social Development, 5*(2–3), 107. https://doi.org/10.5958/2231-458X.2014.00013.X

Han, M., Zhao, H., Ma, X., & Shi, R. (2025). Influencing factors of information security behaviour among college students based on protection motivation theory: Evidence from China. *Frontiers in Public Health, 13*, Article 1677024. https://doi.org/10.3389/fpubh.2025.1677024

Jerusalem, M., & Schwarzer, R. (1981). Self-efficacy as a resource factor in stress appraisal processes. In R. Schwarzer (Ed.), *Self-efficacy: Thought control of action* (pp. 195–213). Hemisphere.

K P, S., & C V., R. (2017). Cyber law awareness among youth of Malappuram district. *IOSR Journal of Humanities and Social Science, 22*(04), 23–30. https://doi.org/10.9790/0837-2204052330

Khan, Z. A., Thakur, V., & Arjun. (2018). Cybercrime awareness among MSW students, School of Social Work, Mangaluru. *Journal of Forensic Sciences & Criminal Investigation, 9* (2). https://doi.org/10.19080/JFSCI.2018.09.555757

Maddux, J. E. (2009). Self-efficacy: The power of believing you can. In S. J. Lopez & C. R. Snyder (Eds.), *Oxford handbook of positive psychology* (2nd ed., pp. 335–343). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780195187243.013.0031

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cybersecurity behaviour among higher education students in Malaysia. *Journal of Information Assurance & Cybersecurity,* 1–13. https://doi.org/10.5171/2017.800299

Munir, A., & Shabir, G. (2018). Social media and cybercrimes in Pakistan: Facts, propaganda, awareness, and legislation. *Global Political Review, 3* (2), 84–97. https://doi.org/10.31703/gpr.2018(III-II).09

Nguyen, M. H., Gruber, J., Fuchs, J., Marler, W., Hunsaker, A., & Hargittai, E. (2020). Changes in digital communication during the COVID-19 global pandemic: Implications for digital inequality and future research. *Social Media + Society, 6* (3). https://doi.org/10.1177/2056305120948255

Pakistan Telecommunication Authority. (2025). Annual report 2024–25. PTA.

Prevention of Electronic Crimes Act (PECA). (2016). Government of Pakistan.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behaviour. *Computers & Security, 28*(8), 816–826. https://doi.org/10.1016/j.cose.2009.05.008

Senthilkumar, K., & Easwaramoorthy, S. (2017). A survey on cybersecurity awareness among college students in Tamil Nadu. *IOP Conference Series: Materials Science and Engineering, 263*, 042043. https://doi.org/10.1088/1757-899X/263/4/042043

Soomro, T. R., & Hussain, M. (2019). Social media-related cybercrimes and techniques for their prevention. *Applied Computer Systems, 24*(1), 9–17. https://doi.org/10.2478/acss-2019-0002

The News International. (2025, January 15). 5-year record of cybercrime complaints with FIA presented in NA. *The News International* https://www.thenews.com.pk/print/1272416-5-year-record-of-cybercrime-complaints-with-fia-presented-in-na

Tonkolu, D. A. (2019). Investigating self-efficacy of cybercrime on social media among university students. Department of Computer Information Systems, NEU.

Zia ul Islam, Khan, M. A., & Zubair, M. (2019). Cybercrime and Pakistan. *Global Political Review, 4*(2), 12–19. https://doi.org/10.31703/gpr.2019(IV-II).02