

Understanding Cyber Crime Awareness Perceptions and Hypothetical Response Among Females Without Victimization Experience

Sufyan Chohan



SCOPUA BOOKS



Understanding Cyber Crime Awareness Perceptions and Hypothetical Response Among Females Without Victimization Experience

By

Sufyan Chohan

Series Title: SCOPUA Books

Scientific Collaborative Online Publishing Universal Academy

i



© SCOPUA Books 2025 | ISBN: 978-627-7898-10-6

Book Title

Understanding Cyber Crime Awareness Perceptions and Hypothetical Response Among Females Without Victimization Experience

Series Name

SCOPIA Books (Email: editor1@books.scopia.com)

Author

Sufyan Chohan

Institute of Social and Cultural Sciences, University of The Punjab,
Pakistan

*Corresponding: sufyanchohan261@gmail.com

Published On

October 08, 2025 (Edition 1)

Publisher

**Scientific Collaborative Online Publishing Universal Academy,
Pakistan**



ISBN: 978-627-7898-10-6

DOI: [10.64060/978-627-7898-10-6](https://doi.org/10.64060/978-627-7898-10-6)



This work is licensed under a Creative Commons Attribution NonCommercial NoDerivatives 4.0 International License. The publisher, the authors, and the editors assume that the advice and information in this book are believed to be true and accurate as of the date of publication. Neither the publisher (Scientific Collaborative Online Publishing Universal Academy, registered and operated from Pakistan) nor the authors nor the editors give a warranty, expressed or implied, concerning the material contained herein or for any errors or omissions that may have been made. SCOPUA (Scientific Collaborative Online Publishing Universal Academy) publisher remains neutral regarding jurisdictional claims in published maps and institutional affiliations.

BISAC

SOC000000, SOC004000, SOC032000

THAMA

JBSF1, JK, JWD



Abstract

This study explored the awareness, perceptions, and hypothetical responses to cybercrime among females who have never experienced victimization, addressing the growing prevalence of cyber threats and the unique vulnerabilities women face online. The focus was on examining how non-victimized females see cyber risk and their awareness levels, and possible reactions toward hypothetical cybercrime cases. The study was qualitative research focused on RAT (Routine Activity Theory), which brings exposure risk through everyday digital activities, into qualitative analysis. And semi-structured interviews were done on the 15 female university students who were purposively sampled to the point of data saturation. Three major themes were identified through thematic analysis; (1) Awareness of Cybercrime, in which most of the general knowledge claimed by participants is rather superficial and usually without any technical detail against some threats like online harassment and scams; (2) Perceptions of Cybercrime, mostly described through media and social influences instead of experiences, while all online behaviors seem cautious and sometimes a little anxious; and (3) Hypothetical Responses to Cybercrime, suggesting a preference for informal support networks like friends and family, coupled with mistrust or unfamiliarity with formal reporting mechanisms. Probing the gap between awareness and action, which can be inferred from the findings, illustrates that limited knowledge is likely to have a protective benefit, but limited preparedness and confidence in institutional support. Therefore, formulations should be made to design any gender-targeted or gender-sensitive technical



empowerment and cybersecurity education programs with possible enhanced technical understanding, leading to encouraging more use of formal reporting avenues within institutions. Future investigations should be implemented on scalable interventions within educational institutions, aimed at equipping females with the necessary skills and resources required for safe navigation of digital spaces.



This Book is dedicated to our beloved parents, whose unwavering love, sacrifices, and prayers have been our greatest source of strength and inspiration. To our family and friends, whose constant encouragement and support have motivated us to persevere through every challenge. And above all, to Allah almighty, whose blessings and guidance have made this achievement possible.



Table of Content

Sr.#	Heading	Page
01	Introduction	01
02	Prior Investigation	08
03	Research Methodology	29
04	Findings and Analysis	34
05	Discussion and Summary	56
06	References	65



Acknowledgements

First and foremost, all praise and gratitude are due to Allah Almighty, the Most Merciful and the Most Compassionate, whose countless blessings and guidance made the completion of this research possible. Without His support, this endeavor would not have been achievable.

We would like to express our sincere gratitude to Dr. Farhan Navid Yousaf, Head of the Department of Criminology, Institute of Social and Cultural Sciences, University of the Punjab, for his continuous support, encouragement, and valuable guidance throughout this research. Our deepest appreciation goes to my supervisor, Dr. Rahla Rahat, for her expert advice, constructive feedback, and unwavering patience, which greatly contributed to the successful completion of this study.

We are profoundly thankful to our parents for their endless love, prayers, and moral support, which have always been a source of strength and motivation. We also extend our heartfelt thanks to our friends who provided encouragement, assistance, and companionship during this journey.

To all who contributed directly or indirectly, their support has been invaluable, and we are truly grateful.

"And whoever relies upon Allah; then He is sufficient for him."

Surah At-Talaq (65:3)



This book project did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. The author declares that she has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this book.



1. INTRODUCTION

Cybercrime is on the rise in the ultra-modern contemporary world, and it's affecting individuals in several ways. In Pakistan, especially within Punjab, the internet and social media are being used by a vast majority. While this carries numerous positives with it, it also has negative effects on females who may not be as smart as they can be about their safety themselves online. This study takes into account females who are never victims of cybercrime. This research provides them, what they know regarding cyber threats, and what actions they would take if they ever found themselves in such a situation (Kaspersky 2019). Most of such females do not know where to make complaints regarding cybercrimes or how to protect themselves online. Through this focus on their knowledge, attitudes, and capacity movements, this analyzes aspirations to communicate the necessity of higher education and recognition concerning cyber safety among younger females in Pakistan.

1.1 Background of the Study

Due to an increasingly digital global landscape, the rise of cybercrime is creating a significant economic and social burden on the international community. It is estimated that the cost associated with cybercrime will hit \$12 trillion in 2025, averaging around \$32 billion a day, while some speculate it could reach \$15.63 trillion by 2029 (Sentinel One, 2024). Indeed, the increase in contemporary threats is underpinned by geopolitical tensions, supply chain complications, and the rapid emergence of technologies such as Generative AI, which criminals can exploit to drive next-level phishing, malware, and deep fake attacks. While attempts to tackle this issue are being



made through large-scale investments in prevention, only an estimated 2% of illicit proceeds from crime were ever recovered by law enforcement, indicating that these threats persist and evolve daily (Crane, 2022).

In Pakistan, like elsewhere in the world, digitalization and flexible work models have created higher risks for businesses and consumers. Malware and phishing attacks extend to more advanced schemes, all climbing up the threat landscape. Ransomware attacks are one of the deepest hits against the manufacturing sector; these kinds of attacks comprise about 70% of detected incidents worldwide. The increase in cyber-enabled frauds and social engineering activities supports urgent requirements for enhancing cybersecurity measures and raising public awareness (Petrosyan, 2024). Studying their level of awareness and cybercrime among females who have never been victims is of prime importance for several reasons. As reliance on digital avenues increases, any user, including those who have yet to fall prey to any cyberattack, is being increasingly targeted by such criminals (Jurgens & Dal Cin, 2025). For females in particular, the acts of cyber threats can take on forms such as cyber harassment or certain kinds of fraud. Any insight into the perception and levels of awareness of non-victimized females can provide great insight into the current gaps in knowledge and can highlight areas where preventive education and strategies may prove most effective. This proactive approach can, in turn, take a step toward building a stronger digital society that equips individuals to protect themselves from emerging cyber threats before actually becoming victims, thus aiding broader crime prevention efforts and reducing the overall impact of cybercrime.



1.2 Awareness and Cognizance Degrees

Within this context, the rapid expansion of internet use in Punjab, Pakistan, has not been seen through a corresponding increase in awareness of cybercrime among females. Most females are blind to cyber winning laws and defensive shields. A (digital right foundation) (2024) report presented delivered that 72% of the Pakistan Researcher females are unaware of to be had cyber legal guidelines and 45% are embarrassed to report cases of cyber harassment, showing an amazing understanding gap and full-scale societal taboo of reporting the crime(Basit et al., 2024). Other research on the degree of knowledge in the context of cybercrimes among pupils also reported that an enormous majority of females possess limited knowledge regarding the subject. They have a glance at confirmed that some of the respondents, an inordinate percentage of graduating females, reported that they only have an average or low level of awareness about cybercrimes.

In Punjab, the situation is particularly problematic. The province has documented a record number of cybercrime cases in the last 5 years through FIA, and one of the most often cited issues has been online harassment, mainly against females(Quresh Researcher et al., 2020). Despite this surge, attempts to educate people about proper net utilization and strategies available to resist cyber attacks were limited. Activities, together with the (cybersecurity) initiative, attempt to plug this knowledge gap through the provision of (cybersecurity) training for females. The program offered a 20-hour (cybersecurity) awareness short course educating trainees on the online abilities needed to safely move around the cyber global (Saleem et al., 2022). Furthermore, corporate entities



such as the Virtual Rights Foundation (VRF) have had a crucial role in averting cyber harassment and marketing women's cyber safety. Since its inception, DRF's cyber-harassment helpline has disposed of over 16,000 cases, providing prison advice and support to victims.

1.3 Cybercrime Prevalence among Educated Young Females

Cybercrime is a significant challenge for educated young females in Pakistan, particularly those who are active on social media and online. According to Finn 2004 10- 15% of university scholars reported passing cyber bullying via hanging emails or dispatches (Faucher et al. 2014) 24.1% of Canadian university scholars reported being victims of cyber bullying over the once time. Also Lindsay & Krysik (2012) 43.3 of a sample of 420 university scholars indicated having suffered from cyber bullying (Dennis, 2019). According to Zalaquett & Chatters (2014), 19 of 613 university scholars reported being victims of cyber bullying; some studies set up as low as 45. In malignancy of acts similar as the Prevention of electronic Crimes Act 2016, reporting charges remain low. Due to social slur ignorance and fear of not being considered serious presently. The cerebral impact is enormous multitudinous female record pressure despair and loss of interest in exploration or art work after being victimized.

1.4 Nature of Cyber Crime Against Females

In Punjab, and indeed Pakistan, cybercrimes against females have grown exponentially in the past few years. In the report of down data (2024) last 5 years, nearly 1.8 million females national have been victims of online abuse and harassment in the form of blackmail, identity theft, and non-consensual sharing of personal images. A tremendous majority of less than



3.5% of suspected offenders were proven guilty reflecting primary failures in the justice system in dealing with such crimes (Khan et al., 2025).

In Punjab, the federal investigation authority (FIA) also reported a rise in cyber crime cases. During the period of 2018-2022 the province recorded 26,924 cases of online fraud 18,851 cases of on line stalking and a pair of 357 cases of online harassment most of which involved lady victims. The advent of technologies that involves synthetic intelligence has also brought about around new types of dangers including deep fake movies and manipulated images which are being extensively used for harassing and defaming females on the internet (Kannathasan & Murugan, 2015). Cyber stalking and Harassment females face constant unwanted attention within the on line environment such as threatening comments and monitoring of their on line activities. A study done in Egypt found that 41.6% of females within the observation had faced cyber violence with 45.3% of them experiencing one or two incidents. Social media became the platform for such harassment and in 92.6% of cases the culprits had been strangers to the victims. ('Cyber sexual harassment: a go-sectional survey over woman university students in higher Egypt' and transformed into published within the global journal of community remedy and Public fitness) (Bhongale 2021).

Cybercrime Wing has found 51,000 complaints regarding deep fakes within the previous 3 years and the complainants have in extensive measure been females. Regardless of the diversity of such offenses there's low awareness of cyber regulations among females in Pakistan. Organizational initiatives such as the Digital Rights foundation (DRF) have played a central role in



addressing on line harassment and fighting for female's virtual safety. DRF's cyber-harassment helpline has responded to over 16,000 complaints since its inception, providing prison guidance and support to the victims. These numbers bring into focus the essential to deal with cybercrimes against females in Pakistan with integrated methods including enhanced awareness, stronger felony frameworks, and stronger law enforcement activity.

1.5 Significance of the Study

Vulnerabilities in Cybercrime maximum in females of Punjab who make use of the internet for getting to explore opportunities and social networking Nevertheless, they're not knowledgeable about the risks that lie on the internet. Females, especially students, are more liable to cybercrime because they may lack proper records regarding online protection (Aslam et al., 2023). Hackers, blackmailers, and harassers on the internet target females normally the usage of faux debts, hacked profiles, or leaked private records. Most females fail to report such crimes because of fear, disgrace, or family stress. This necessitates the understanding of the way properly-ready females are to deal with such threats even earlier than encounters. Causes and outcomes of Cybercrime in opposition to females Cybercrime had intense emotional, social, and mental impacts on females. Even though they'll in no way had the enjoy worry of being a victim can have an effect on their freedom and self belief on line (Riaz, 2021). Alliances of cybercrime can come via lack of awareness, irrelevant privacy settings, susceptible passwords, and the open sharing of private information. The impact can be strain, depression, damage to reputation, or halting training or social life. Reading



those issues assists in figuring out manner of safeguarding females and securing the internet for them. Significance for coverage makers and training Society it's far large for schools, universities, and government corporations in Punjab to know how ready young females are to cope with threats from the internet (The Broadband Commission for Digital Development, 2024). If we're aware about what statistics and help they are missing, Researcher is able to assist with schooling, statistics dissemination campaigns, and more effective cyber legislation. This study can inform policymakers to prioritize female digital protection and give a boost to cybercrime legislation. It may additionally enable females to safely get admission to the net, with more self assurance. In the end a safer online environment for females manner a stronger more equitable digital community.

1.6 Attitudes and Behavioral Responses

Attitudes closer to cybercrime without delay have an effect on the manner where in people react to possible threats. This similarly highlights the need for emotional intelligence and sensitivity in stopping cybercrime. Also the absence of proactive reporting habits amongst students shows that there's a demand to promote a way of life for encouraging vigilance and well timed action towards cyber assaults (Shahzad, 2023).

Gender Dynamics in Cyber safety Engagement: In 2023-2024 Jane Frankland a cybersecurity expert and LinkedIn Top Voice who has contributed insights on gender disparity in the UK's cybersecurity industry and have a look at carried out inside the United Kingdom investigated gender variation in cyber security behaviors. Results showed that females tended to use social circles for advice greater than online sources which men used



extra frequently. This dependence should restriction females' get admission to thorough cyber safety data which might have an impact on their exercise of on line safety.

Educational Intercede and Their Effect: The Cyber Delegates initiative of the Telangana state in India is a superb example of forward wondering training. Launched with the growing fees of cybercrime, it had extra than 3,000 students trained in the first year alone to become aware of and respond to cyber threats. Such programs show the effectiveness of systematized schooling in growing the notice and reaction to cybercrime among youngsters.

Organization and Authorities Measures: a number of organizations and government businesses have initiated programs to counter cybercrime and growth focus Pakistan: The national Cyber Crime investigation organization (NCCIA) turned into set up to cope with cyber threats and shield digital rights. The Punjab fee at the popularity of females (PCSW) works in partnership with diverse stakeholders to ensure females' protection on the internet and gives substances which includes a 24/7 helpline for reporting harassment

2. PRIOR INVESTIGATION

Cybercrime poses an increasing danger within the digital era, particularly to female university college students who are constant net consumers. Concurrently, as studies have researched cybercrime victimization, less has been centered on female students who have not yet no longer been victims of cybercrime but could be vulnerable. This literature review discusses their readiness, attitudes, and capability reactions to cyber-attacks, basing it on research work in Nigeria, Pakistan, and broader cyber protection consciousness studies.



2.1 Concept and Types of Cybercrime

Cybercrime is becoming a critical issue around the globe as it increases considerably with advancements in technology. Researchers define cybercrime as a combination of illegal activities performed digitally through identity theft, cyber harassment, phishing, and online fraud (Researcher & Liu, 2021). The rate at which cybercrime has gone up globally is at a level where it affects individuals, organizations, and governments. However, on a personal level, cyberstalking and online harassment are two forms of cybercrimes targeting women (Singh, 2025). However, there are not many studies on awareness and perception regarding cybercrime among females who have not been victimized.

The studies that were conducted revealed diverse findings regarding the knowledge of cybercrime among women. Although the females in the study conducted by Pandey & Kapoor (2025) were heavy users of the internet, they were not cognitively aware of the threats, dangers posed to them and their preventive measures against cybercrime. They attributed this lack of awareness to digital illiteracy and scant familiarity with cybersecurity instruction. On the contrary, Kuzior et al. (2024) reported more awareness among educated urban females, thus indicating that one of the socio-demographic factors affecting knowledge about the cybercrime phenomenon is education and urban residence. Hence, the recognition becomes a measure of a context-dependent phenomenon or is not uniform across individuals. Perceptions concerning the risk of cybercrime may differ among females who have never experienced victimization. Chen et al. (2023) noted that many females tend to believe that they are not susceptible to any



victimization by cybercrime since it is generally seen as something that happens to other people but not to them. This way of thinking is an optimistic bias, so they become complacent about caring behaviors. Griffiths (2025) observed the same trend regarding the perception of low chances of becoming victims of cybercrimes, while most females admit to acknowledging existing cyber threats; hence, the motivation to take prevention measures would be negatively affected. These studies thus placed a very sharp focus on the critical disconnect between awareness and personal perceived risk.

Another focus of the study included the hypothetical responses and preventive measures that females would like to consider effective. Proactive strategies like using strong passwords, avoiding suspicious links, and regularly updating software were emphasized by several scholars (Kala, 2023). Wilk (2021) revealed that even though females were aware of these measures in theory, the measures were not implemented in practice. This was due to the general attribution of understanding and ability to implement actions to a lack of confidence regarding skills and the complexity of cybersecurity tools. In addition, social and cultural barriers did not encourage females to represent or disclose threats online and accordingly approach the use and methods of effective responses (Council of Europe, 2023).

For example, the Routine Activity Theory (Cohen & Felson, 1979) was used to demonstrate the extent to which online patterns of everyday conduct influenced an individual encountering cyber risk (Vakhitova, 2025). Applying this theory, researchers argue that the higher the level of online activity amongst females, the more exposure they will have to



cyber threats; however, the larger the opportunity for learning about the prevention of these threats exists (Nahar & Emran, 2021). Protection Motivation Theory has also been used to show how perceived severity and vulnerability influence the adoption of cybersecurity-related behaviors by females (Wikström, 2009). These theories have resulted in finding interesting psychological and behavioral aspects regarding the prevention of cybercrime.

Most studies utilized a quantitative survey methodologically to measure the awareness concerning perceptions and behaviors related to cybercrime. For example, across-sectional survey was conducted by Yar (2005) among university females to gauge knowledge and attitudes toward cyber threats. Qualitative (interviews and focus groups) were less used but gave an even deeper insight into personal experiences and cultural influences (Madarie et al., 2025). The richness of understanding of the phenomenon thus presented showed the need for mixed-method approaches to be used in capturing the complexity of awareness around cybercrime. According to the reviewed literature, much-needed attention has been given to education and awareness programs for females. Several authors further recommended integrating cybersecurity programs in school curricula as well as community outreach programs for improving digital literacy and empowering females to protect themselves, among others (Artfield, 2015). In addition, the literature emphasized the need for culture-specific intervention strategies that would tackle social barriers and promote open discussion on cyber risks (Caeiro, 2024). This would also be in tandem with other broader efforts to define and renew gender-specific responses in cybersecurity policy and practice.



However, the review demonstrated that while awareness of cybercrime among females has increased, gaps still exist in perception and preventive behaviors toward it. The literature revealed that very socio-demographic as well as psychological-theoretical and cultural factors shape awareness about and response to cybercrime. More future research should be directed to non-victims by mixed methods, coupled with technological innovations, for effective, inclusive prevention

2.2. Awareness Level among Females

Garba et al. (2020) carried out a quantitative study at Yobe National College, Nigeria, to appreciate the level of cybersecurity awareness among students. Their results showed that while students had some rudimentary knowledge of cyber threats, many of them demonstrated a lack of initiating proactive, everyday security-related behavior, as password management and phishing awareness. This only showed that university students were often not ready to thwart possible attacks, even when they had not experienced cybercrimes. The study, therefore, drew attention to the wide gap between theoretical knowledge and the practicality of cybersecurity behavior by the young-adult population in academic institutions (Abu-Bakr, 2020). Khalid et al. (2022) examined cybercrime awareness among university students in Sindh, Pakistan. Cyber bullying was found to have low awareness, and preventive knowledge was almost non-existent. Many students were unaware of formal reporting procedures, demonstrating a gap between awareness of cyber threats and knowing how to respond effectively. This gap implied that students remained vulnerable, albeit with some level of threat recognition; hence,



the need for an education program that covers the identification and response to cybercrime.

Aleem (2022) viewed cybercrime from a feminist lens, specifically regarding the experiences of female college students in Pakistan. The study found that although most female students were concerned about online harassment, they had little faith in the contemporary system of support. Despite feeling that they had not been personally victimized by any acts of cybercrime, these females warmly expressed their grave concern over intrusions of privacy, impersonation, and cyberstalking. The study then reiterated how the very anxiety about cyber threats was determining the very behavior of females online, some limiting their presence to reduce risks, while others dismissed threats simply because they had not experienced them. Khan and Ahmed added that there is an exigent need for gender-sensitive cybersecurity education that could focus on some specific risks to women, such as non-consensual image sharing and harassment.

There is also some research showing that those who have experienced cybercrime in the past do not perceive themselves to be vulnerable anymore which causes a kind of complacency (Tarar et al., 2021). This path of complacency actually gives a reactive profile to the majority of students, who are usually found adopting protective measures post attack rather than on a proactive basis. Such behaviors would indeed heighten the chances of their first-time victimization. Nevertheless, the preparedness could be enhanced through implementation awareness programs. Zahoor & Razi, (2020) vividly asserted that workshops in cyber protection and simulation can greatly improve students' awareness of cyber threats and response



strategies, thus emphasizing an appreciation for such proactive educational interventions.

For female students in particular this topic (trainings-on-gender-specific online risks) had a positive effect on guiding them against these risks. Rafaqat et al., (2024) pointed out those training women concerning specific issues, such as online harassment and image-based abuse was critical in allowing them to recognize and resist such threats. The lack of formal courses on cybersecurity in various universities was a recurring narrative. Shaikh et al. (2022) stated that many of the universities neglected to introduce this dimension in their curriculum on cybercrime prevention, hence being misguided by informal sources of information. This big gap was particularly worrying to female students who suffered unique threats yet had no guidance and lack of institutional support. The study also established that there was limited enforcement of the same rules and insufficiently effective reporting mechanisms. According to Khan and Ahmed (2022), social stigma and doubt over the efficiency of legal means made female students in Pakistan reluctant to report cybercrimes impeding their access to justice and sustaining their vulnerability. Institutional support structures should be strengthened to address such barriers and enhance regarding reporting. The literature indicates that risk perceptions sometimes being overestimated by female college students who were not victimized but without the presence of threat recognition opportunity, preparation, and institute support they remained being vulnerable. While some of these evidences coming from Nigeria and Pakistan as well as other cyberspace researchers cast light on a standard need for pre-emptive



training, gender-sensitive education, and better channels for reporting. Future study is needed to explore how universities can equip female students with more knowledge and resources to be able to prevent cybercrime prior to them being victimized. Anwar et al., (2017) examined the gender differences in cybersecurity concerns among university students within West Africa. They discovered that while male and female university students possessed similar basic knowledge of cyber threats, females showed lack of confidence in the management of such risks. The lower confidence among females was attributed to inadequate technical skills and less exposure to education opportunities. Thus, it indicates that female students that have never experienced cybercrime are vulnerable mainly due to lack of exposure and support systems. In the South Asian context, Javaher Researcher et al., (2024) studied digital literacy and cybercrime susceptibility among college students from Pakistan and India. Their research highlighted the fact that insufficient digital literacy contributed towards giving increased vulnerability particularly amongst females. Thus, they advocated inclusion of digital skills training as part of educational curricula, augmenting students' capacity to recognize and respond to cyber threats.

Summarily, all these studies testified to a consistent pattern; while there was a general awareness of cyber threats within university students, a pertinent gap in the areas of preventive knowledge, confidence, and institutional support existed most markedly for females. Research has strongly recommended that bridging such gaps with gender-sensitive education, proactive training, and well-defined reporting mechanisms stands as a



means towards empowerment of female students and diminished risk of cyber victimization.

2.3 Perceptions Among Females

Bada & Nurse, (2020) studied the psychological implications that cybercrime fear has on female college students; according to such study, anxiety on the part of students who have never been victims of cybercrime tends to occur as a result of perceived vulnerability, whereby some girls end up hiding their online activities or avoiding certain sites altogether. The study essayed the psychological burden associated with waiting in the anticipation of being victimized without ever being a victim of cybercrime. The study also found in correspondence with Kraemer et al., (2009), which studied the response of females to cyber threats based on gender, that females were found to be more concerned with issues related to privacy but was less likely to take the initiative of adopting proactive technical measures like encryption or firewall use. There has been a clear difference in regard to concern and preventive behavior resulting in a gap in knowledge in preparedness, as mentioned above, among female undergraduates before falling victim to cybercrime.

According to Baraković & Husić, (2022), a quantitative study on cyber security behavior among wireless-year female undergraduates in America was carried out. The results showed that less than 20 percent of respondents utilized two-factor authentication, while password reuse dominated. Most of the respondents give them the impression that they were not aware of such habits but rather fell prey to cyber threats. This proves that experience with cybercrime has reduced the perception of risk and security practices. However, Khan, (2022) reviewed



the concept of the digital divide in tertiary education in Pakistan. The researcher noted that although women now have relatively higher access to digital devices, their knowledge on cybercrime and self-protective behavior is still very low. This part shows that even technical education doesn't guarantee practical capability in cybersecurity competence, as it possesses some gender-associated stereotypes and barriers within the education environment. Aslam et al., (2023) experimentally tested the willingness of females in Pakistan to report cyber attacks among students, as some barriers to reporting included fear of social stigma, distrust of law enforcement agencies, and concerns about victim-blaming. First-time victims are trapped within these social and institutional constraints that must, therefore, point out the need for awareness and action-oriented support mechanisms.

Effectiveness of workshops on different aspects of gender-sensitive cybersecurity directed towards female university students was evaluated in Poulpunitha et al., (2020). This shows that addressing destruction of non-consensually shared images to be improved greatly the readiness and risk awareness of each participant. This once more demonstrates the worth of tailor-made educational intervention in building confidence and preparedness before any such time occurs. Chaudhry et al., (2023) reviewed differences in behavior of university students at the risk of having encountered cybercrime as opposed to those who had not. Non-victimized students, for example, demonstrated weaker defensive behaviors, showed lower motivation for change, and appeared less inclined to enter into some form of change. The reactive mindset that seemed to exist whereby preventive action was taken in victimization further



emphasized the need for proactive education strategies. Alnajim et al., (2023) conducted a cross-sectional survey among Spanish adolescents, reporting that female respondents were more likely than male respondents to worry about and perceive risks involving online victimization. Despite this heightened concern, females' perceptions often led them to view greater risk than they experienced, which may have had an effect on their behaviors and coping mechanisms online. This difference in risk perception and worry by gender suggested that females might be exaggerating certain cyber threats, yet lacked adequate real skills sufficient to reduce them into manageable proportions.

Mishra et al., (2022) has undertaken the work of studying cyber security awareness among Indian female university students. The study found that students were generally aware of password and social media security, but there were gaps in knowledge concerning other terms associated with cybercrime, such as phishing, cyber bullying, or browser security. Therefore, this gap in perception versus practice puts them at a greater risk, considering their limited experiences with direct cybercrimes. The reports bore indications that cognitive aspects such as emotional tolls of fear and anxiety with danger in cyberspace highly affect performance on the internet but do not necessarily transform into meaningful practices in cybersecurity. Further, social and cultural barriers such as stigma and lack of trust in institutional authorities keep victims from reporting or taking proactive measures. Research showed a critical need for gender-sensitive cybersecurity education programs. Psychological and practical education addressing the prevention of cybercrimes. Workshops and campaigns that are



tailored have been shown to improve readiness and confidence among female students with know-how and skills for proactive protection. Also, it was suggested that institutions develop better reporting mechanisms and that there should be efforts to reduce social stigma so as to encourage the timely seeking of assistance.

Rasheed et al., (2024) target female university college students at cities in India and their vulnerability through social media use. Most members admit over-sharing their personal information while counting solely on default privacy settings. Illusion of security, mixed with lack of experience with cyber threats, makes them particularly vulnerable to impersonation and stalking. Uda Researcher & Sharma, (2025), surveying cybersecurity policies across Nigerian universities, uncovered an alarming loss of gender-specific wireless strategy. Most of the organizations reported common awareness scheme but did not include a wireless approach for female college students. The absence of inclusive-specific policy and representation reduces the efficacy of modern interventions for unaware female students. Chaudhry, (2024) studied cyber ethics education in Pakistan and its correlation with the critical age of younger females. Their observation endorsed that the absent majority of students was even oblivious to their online rights or ethical boundaries about their behaviors online. The absence of formal training on this area led to poor decision making and susceptibility to cyber victimization. An international UNESCO (2023) report surveyed more than 30 countries about their females' online protection and empowerment. The wiwireless observed cultural restrictions, linguistic barriers, and lack of localized materials contributing to inadequate



cybersecurity readiness in young females. It suggested the utilization of network-based applications and culturally relevant ones to augment readiness and resilience. Dwivedi Researcher et al., (2021) investigated preventive cybersecurity education at universities in South Asia and concluded that the development of gender-inclusive curriculum material increases both participation and retention of lady students. Moreover intuitive sporting activities along with realistic case studies and scenario-based completely learning lead to quantifiable improvements of cognizance and protective behaviors

Balaj Researcher et al., (2023) examined the cyber readiness of Nigerian lady undergraduates. The wireless result revealed that even though many participants had high usage of smartphones and social media, far fewer understood threats like malware or phishing. Maximum do not use precautionary measures, including password managers or easy practices, representing a gap in preventive habits among one never exposed to a cyberattack. Com Digful, (2022) described the perceptions of Pakistan Researcher lady students on security with social media. The tester noted that people who had never experienced cybercrime felt that being online "cautious" was actually wiser enough protection. This hardwired overconfidence, combined with shared images of themselves and public profiles, increased their risks without them being aware. Dennis, (2019) investigated university-level cybersecurity uses in Ghana and their magic to female university students. Institutional initiatives notwithstanding, attendance by females decreased into poor, wificaly amongst females who had by no means experienced cyber threats. Those scholars thought cybersecurity became a male-centric occupation or irrelevant to



their scholarly recognition, in much the same way as it decreased their participation.

Researcher & Liu, (2021) found in their investigation into readiness for cyber-attacks reported by female students in Lahore, Pakistan, that private reports concerning cyber harassment mainly led to behavior change through wireless. Those reports mostly lead to preemptive actions, such as reporting suspect messages or setting privacy settings aside from those without such reports. Petrosyan, (2024) was based on female students' willingness to withstand cyber wire capping in co-academic campuses. The domestic results showed that even among students who were not trained in cybercrime, the fear of being judged or mocked mostly kept them from seeking help or discussing openly cyber security concerns. Riaz, (2021) surveyed Southeast Asian university college students and discovered that most woman authors who have never fallen victim to cybercrimes underestimated their risks. The majority of them actuated their security settings by default and had no knowledge of email spoofing or social engineering processes, signifying the dangers that lay in ignorance and complacency. In terms of females in colleges across Pakistan, Garba et al., (2020) evaluated the extent of effectiveness of virtual literacy activities. The examination revealed that even when applications were available, participation remained low among female college students who considered that there were no adverse reports beyond personal accounts. Jurgens & Dal Cin, (2025) studied female ideas on institutional assistance in Bangladesh's universities. The overwhelming majority were oblivious to the methods of digital grievance cells or online safety officers. This ignorance became especially widespread



among students never experiencing cyber harassment. Kala, (2023) investigated the safety behavior of female university students in using the mobile applications. Most of them visit all app permissions without evaluation. Among people who never became victims of information breaches, there was low understanding of consequences afterward. Pandey & Kapoor, (2025) studied on cyber grooms' awareness on Indian adolescent females. Most of these were found to believe others about unknowingly divulging to strangers, through social media Wi-Fi, due to less exposure and concept of threat, if they ever faced an adverse online behavior. Bada & Nurse, (2020) studied the influence of own family background on female students with respect to cyber hygiene. Those who depended on family advice often missed contemporary knowledge on digital threats, as well as very low knowledge of technology, which made them less defendable among students lacking previous exposure to cybercrime.

2.4 Hypothetical response to Cyber Crime

Aleem, (2022) examined young females susceptibility to financial cyber fraud. Students who had never encountered Wi-FResearcher wireless swindles had been more trusting of e-commerce infrastructures and less likely to WI-FResearcher fearless fee websites, resulting in capacity exposure to economic wireless exploitation. Basit et al., (2024) highlighted the role of peer tradition in influencing cybersecurity behavior. Female students who had never been cyber victims consistently adopted informal protection behavior if their peers did; perpetuating communal complacency Underreporting of cyber-attacks in Pakistan Researcher universities was explored by Shabbir & Adnan, (2025). Female students, particularly those



not exposed to Cybercrime, were unaware of the process or institutions involved in wi-filing a complaint, indicative of systemic consciousness gaps.

In & Malik, (2022) investigated how data of net monitoring Wi-FResearcher consumer conduct. Even in the absence of direct experience, feminine scholars changed online behavior (avoiding favorable seek or content material) following finding out that they may be monitored. Bhutta and Hashm Researcher (2023) investigated the cyber extortion fear among Pakistan's female clinical students. Despite no previous occurrences, there was student expressed situation regarding non-public photo leaks and the implementation of strategies such as avoiding cloud backups or turning off digital camera permissions. Javaher Researcher et al., (2024) tested virtual resilience among Pakistan Researcher female college students with hypothetical threat simulations. Individuals who never experienced cybercrime struggled with trouble-wiwireless and emotional law when faced with simulated attacks, suggesting low preparedness. Kala, (2023) researched the role of online communities in educating females on cyber safety lady college students who engaged in digital feminist forums showed higher levels of understanding and more active protection measures, even though they had not faced any threats wireless hand. This perception is important due to the fact worry of cybercrime can affect on line conduct. Some female students might also restrict their virtual presence to avoid risks, at the same time as others may additionally underestimate threats because of a lack of direct revel in. They have a look at emphasized the want for gender-touchy cybersecurity education to empower females with preventive techniques.



Garba et al., (2020) on cyber protection behaviors observed that many college students' best undertake shielding measures after experiencing an assault, in preference to preemptively. This reactive attitude leaves them at risk of web-first-time victimization. However, studies additionally indicate that consciousness applications can improve preparedness. For example, simulations and cyber protection workshops had been powerful in growing threat reputation and reaction techniques amongst college students (Kaspersky, 2019). Female students, specially, we-fit from schooling that addresses gender-unique wireless dangers, along with non-consensual photo sharing and online harassment. A commonplace theme across research is the shortage of based cyber safety education in universities. Many institutions do now not integrate cybercrime prevention into their curricula, leaving college students to depend on informal assets for statistics (Kuzior et al., 2024). This gap is especially regarding for female students, who may additionally face precise threats but lack tailored steerage.

Moreover, consider in regulation enforcement and reporting mechanisms is low. In Pakistan, female students regularly hesitate to record cybercrimes due to fear of social stigma or useless felony recourse (Mishra et al., 2022). Strengthening institutional guide structures and selling cybercrime consciousness campaigns ought to mitigate these challenges. Woman college students who have never experienced cybercrime can also underestimate their hazard, yet they stay inclined because of gaps in recognition, preparedness, and institutional assist. Research from Nigeria, Pakistan, and broader cyber security studies highlight the need for proactive education, gender-touchy schooling, and stronger reporting



mechanisms. Destiny studies need to discover how universities can better equip woman students with the information and tools to prevent cybercrime before victimization occurs. Chaudhry (2024) investigated the virtual divide in higher education and its effects on cybersecurity readiness. His take a look at indicated that although females students in Pakistan have growing get right of entry to digital devices, their awareness of cybercrime and shielding behaviors stays low. This example is worsened via cultural taboos that discourage open discussions approximately online harassment or fraud, leaving many students remote in their stories.

Aleem, (2022) tested the willingness of lady students in Pakistan to Wi-FResearcher cyber incidents. Their web-findings highlighted that many females avoided reporting because of worry of social stigma, mistrust in law enforcement, and issues over victim-blaming. Those social and institutional barriers make it Wi-FResearcher for wirelesses-time sufferers to searching for wireless help, further emphasizing the sign wireless of preemptive recognition and aid. These wireless endings we-firm the price of gender-sensitive academic tasks to construct self belief and readiness earlier than any incident happens. Aslam et al., (2023) focused on woman university college students in city India and their vulnerability thru social media use. Many members admitted to oversharing personal information and relying entirely on default privacy settings. This fake experience of safety, compounded by way of inexperience with cyber threats, made them specially liable to impersonation and stalking. Vakhitova, (2025) studied cybersecurity policies in Nigerian universities and discovered a vast loss of gender-wi-FResearcher wireless strategies.



Maximum establishments had general awareness programs but didn't cope with the specific wireless worries of lady college students. This lack of inclusive policy and illustration reduces the effectiveness of modern interventions for unexposed female students.

Wikström, (2009) looked at cyber ethics training in Pakistan and its impact on younger females. Their facts indicated that non-public reports with cyber harassment frequently induced behavioral modify wireless, at the same time as the ones without such studies not often took preemptive steps which include reporting suspicious messages or adjusting privateness settings. They tended to use default protection settings and lacked consciousness approximately email spoofing wirelessness or social engineering procedures, demonstrating the dangers of inexperience and complacency. Uda Researcher & Sharma, (2025) assessed the effectiveness of virtual literacy tasks in female's colleges throughout Pakistan. The look at concluded that even as applications existed, participation become low amongst females college students who perceived themselves as safe due to a lack of negative beyond reports. Zahoor & Razi, (2020) explored woman college students' perceptions of institutional help in Bangladesh Researcher universities. Many have been blind to the lifestyles of digital grievance cells or online protection officials. This lack of knowledge became especially commonplace amongst students who had in no way experienced cyber harassment. Rafaqat et al., (2024) investigated the safety conduct of female college students while the use of cell packages. Many users frequent all app permissions without assessment. Amongst individuals who had now not been sufferers of records breaches, there was little



understanding of the effects of such actions. Quresh Researcher et al., (2020) studied awareness of cyber grooming amongst adolescent females in India. They located that people who had by no means encountered predatory behavior online have been more likely to trust unknown customers, Wi-FResearcher on social media, due to a loss of exposure and threat perception. Javaher Researcher et al., (2024) tested the position of own family have an effect on female college students' cyber hygiene. people who depended on own family guidance frequently lacked contemporary know-how of digital threats and had minimal technical skills, leading to weaker defenses among college students without a earlier cybercrime publicity.

2.5 Theoretical Framework

The theoretical background for this study rests on Routine Activity Theory as a theoretical framework, which is one of the leading, although not the only, criminological theories on how crimes occur. It was originally developed by Cohen and Felson (1979) to explain the convergence of three elements that lead to crime: motivated offenders, suitable targets, and absence of capable guardians. RAT posits that crime occurs when these three elements coincide as to time and space, thereby emphasizing situational nature of victimization.

Adaptation of the RAT has thus developed around the special case of cyberspace; here physical proximity is not necessary for crime to occur. Generally referred to as Cyber-Routine Activity Theory (CRAT), this adaption captures the intensity with which motivated offenders exploit the opportunities by which users enact their everyday online behaviors, targeting those who perform routine digital activities without having sufficient protection or awareness (Bada & Nurse, 2020). Unlike crimes



that are perpetrated in a physical environment, cybercrimes occur asynchronously and over great distances. The deterrent effect of capable guardians (such as witnesses) is diminished because of anonymity and invisibility associated with digital oppositions (Oxford Research Encyclopedias, 2025).

It allows interpretation of RAT as applied to cybervictimization against females who had never been victimized. The type of everyday behavior such as using social media or communicative purposes and sharing information online exposes them to online threats. According to the theory, engaging in predictive online routines without enough protection makes those females become suitable targets for cybercriminals (Basit et al., 2024). Absence of capable guardianship in cyberspace could be taken to denote either inadequate technical safeguards (e.g., strong passwords, two-factor authentication) or those social support systems failing which attacks could have been institutionalized or mitigated in their effect (UNODC 2018).

Lifestyle-Routine Activity Theory (L-RAT), which extends RAT, asserts the impact of personal life choices and behavior patterns on vulnerability to crime, including cybercrime (Scholar Online, 2024). This model would help explain an increase in risk from victimization among females who usually spend a lot of time online or share a lot of personal information, even though they had not been previously victimized (Griffiths, 2025).

Using RAT and its cyber-adapted variants, this study will analyze how females' routine digital activities and the presence or absence of protective factors contribute to indicated and actual risk of cybercrime. Also to be considered is the



importance of enhancing capable guardianship through education, awareness, and technological safeguards in reducing vulnerability. This theoretical lens thus supports the focus of the study on awareness, perceptions, and possible responses to cybercrime, framing victimization risk as a function of one's routine behaviors and protective mechanisms in the digital age.

3. RESEARCH METHODOLOGY

This administration information the method used in carrying out this looks at titled “Understanding Cybercrime Awareness Perceptions and Hypothetical Responses among females Without Victimization Experience”, this research delves into the experience, attitudes, and opinions of female students who have never been victims of cybercrime. Given that the concerns are subjective and exploratory in nature, the research transformed into qualitative. This bankruptcy describes the studies technique, sampling technique, information series process, and analytical approach that obey to the research hassle (Rafaqat et al., 2024).

3.1 Research Design

In qualitative research, research design refers to the overall strategy that a researcher uses to integrate the different components of a study in a coherent and logical way. It ensures that the research question is effectively addressed using methods that explore meanings, experiences, and understanding from the participant's point of view (Griffiths, 2025). In this research, a qualitative studies design was utilized to examine the experiences. Qualitative research is sought after in the examiner of complex social phenomena to assist benefit deeper understanding into how humans make sense of their narratives. Here, the focus was on investigating female



students' readiness for cybercrime, their understanding of virtual risks, and their hypothetical behavior in cybercrime scenarios. Unlike the method applied to measure phenomena, with the aim of measuring and generalizing, this qualitative study sought to discover the meanings given to their reviews by members. This approach permitted taking pictures nuanced perspectives and investigating themes that might not have been apparent through dependent surveys or statistical analysis.

3.2 Research Setting

Research setting in qualitative research refers to the physical, social, or cultural environment where the study takes place. It is the place or context in which researchers interact with participants to collect data. These research were selected because they represent a population with regular internet access and exposure to digital platforms, making them relevant to the study of cybercrime awareness and response (Vakhitova, 2025). Data was collected from universities, workplace, and through online platforms to ensure diverse participation while maintaining the key criterion that respondents had never personally experienced cyber victimization. To capture their voices, Researchers visited classrooms, university libraries, and work places where female students and professionals worked and studied. Many were curious when approached, asking questions like, “Why only those who have never been victimized?” This sparked meaningful conversations and brought attention to a rarely explored group those at risk but unaware. Online platforms were also used to reach participants who preferred digital communication. Carefully designed consent forms and questionnaires were shared through email



and messaging apps, ensuring accessibility while maintaining confidentiality.

3.3 Sampling Technique

A sampling technique in qualitative research is the method used to select people or groups who will take part in the study. These participants are chosen because they have experience, knowledge, or insight about the topic being studied (Singh, 2025). In designing this research, one of the most important steps was selecting the right Participants those whose experiences could offer valuable insights into the awareness, perception, and hypothetical responses to cybercrime among females who have never been victimized. But how could Researcher find them? Instead of randomly approaching every female Researchers came across, Researchers decided to use a purposive sampling technique. This method allowed me to intentionally select participants who fit the specific criteria of his study: females aged 18 and above, who use the internet regularly but have never experienced any form of cybercrime. Some participants were found through referrals friends and classmates who shared the link to his questionnaire or introduced me to others who met the criteria. Researcher also used online platforms such as Whatsapp, Instagram, and university mailing lists to share a digital version of the questionnaire, making it easier for busy or distant participants to join the study.

The purposive sampling approach gave me the freedom to choose respondents who were most relevant to the research objectives. This was not about reaching thousands of people; it was about reaching the right people those whose insights could help paint a clearer picture of how females who have never



been harmed online think, feel, and would possibly act if ever faced with a cyber threat. Researchers reached out 35 different females by using this method and during this some are not relevant to the study and some are canceling the meeting on time some are busy and not available on time of commencement and after taking interview of 15 females with both student and workplace background due to saturation of answers after 15 females.

3.4 Data Collection

Data collection in qualitative research means gathering information from people to understand their thoughts, feelings, experiences, or behaviors in detail. Common Ways to Collect Data: Interviews (Asking people questions in person or online). Focus Groups (Talking with a small group about a topic). Researcher chose to collect data using a structured questionnaire but in depth and open ended a tool that would allow me to gather organized and comparable responses across a wide range of participants. But this wasn't just about handing out forms or links. It was about creating a safe and respectful space where participants felt comfortable sharing their views, even if they hadn't faced cybercrime themselves.

The questionnaire was carefully designed in three sections. The first part focused on awareness asking participants about their knowledge of cybercrime types, laws, and digital safety. The second section explored their perceptions, such as how serious they believed the threat of cybercrime to be, and who they thought was most vulnerable. The final section looked at their hypothetical responses, including whether they would report a cyber incident, seek help, or change their behavior if targeted online. Researcher interview participant in two main ways: in



face to face and online. On university campuses and in office settings, Researcher approached participants directly, briefly explaining the purpose of the study and ensuring them that their identities would remain confidential. Researcher interview them in quiet corners of classrooms or staff rooms, libraries and restaurants while others preferred to do it in university open quite place.

3.5 Data Analysis Process

Analysis was utilized to analyze the interview facts. This method entails identifying, exploring, and interpreting meanings of styles in the records. After weeks of careful planning, designing, and collecting responses from the right participants Researcher found ourselves looking at a collection of completed interviews each one filled with the voices of females who had never experienced cybercrime but had something important to say about it. These papers and online forms, though silent, carried valuable information that needed to be carefully unpacked, analyzed, and brought to life. Next descriptive analysis Using SPSS, Researcher calculated frequencies, percentages, and means to understand the general trends. How many participants had basic awareness of cybercrime? What percentage believed cybercrime was a serious issue for females in Pakistan? How many said they would report an incident if targeted online? These numbers started telling a story one that reflected confidence and confusion, awareness and uncertainty.

3.6 Ethical Consideration:

Ethical consideration in qualitative research means protecting the rights, privacy, and well-being of the people who take part in the study.



- Informed Consent Participants must agree to join the study willingly
- Their personal information must be kept private.
- Treating participants with care and telling the truth.
- Making sure the research does not hurt anyone emotionally or physically.
- The goal is to do research in a fair, respectful, and responsible way.

From the very beginning of this research journey, Researcher understood that working with real people listening to their thoughts, asking about their views, and exploring sensitive topics like cybercrime required more than just a questionnaire. It required care, respect, and responsibility. That's where ethical considerations became a guiding light throughout every stage of the study.

4. FINDINGS AND ANALYSIS

The results of this study present a complex multi-faceted understanding of cybercrime by those women who have never personally experienced being victimized. Analysis of the data involved an in-depth examination of the interview responses of a pool of 15 female students who were chosen from an initial sample of 30 participants after reaching saturation following interviews. The analysis sought patterns and divergences in awareness, perceptions, and hypothetical responses regarding cybercrime. Results from the data analysis suggested that participants' levels of awareness vary greatly in relation to their age, background education, and exposure to the digital world. Almost all participants were somewhat aware of the common cyber threats of harassment, scams, and breaches of privacy. However, understanding was often shallow; in particular, the



participants seemed largely unaware of specific mechanisms of cybercrimes or technologies to counter them. Participants' perceptions of risk of cybercrime, it appeared, were informed by the media, their social circles, and hearsay rather than driven by their own experiences. Nevertheless, most were concerned to some degree and seemed to exercise guardedness-a manifestation of self-protection damage stemming from their limited awareness. Thus, their awareness-not extensive in its coverage-still exerts a positive influence on cautious online behavior.

In discussing possible responses to some theoretical cybercrime scenarios, informal support options, such as friends and family, were generally favored over formal legal or institutional avenues. This turn to informal systems indicates either a lack of trust or a lack of familiarity with official reporting mechanisms or legal remedies. From here, the data emphasized a critical schism between awareness and the initiation of action. Thus, the data recommends that more intensified education and empowerment strategies be adopted so that women can protect themselves in Google spaces.

Table 4.1: *Demographic Profile of Participants*

Sr.	NAME	AGE	EDUCATION	BACKGROUND
1.	Amina	26	BS. Physiotherapy	Working females
2.	Hareem	22	BS. E-Commerce	Student
3.	Nimra	23	BS. Sociology	Student
4.	Naimal	20	BS. Mathematics	Student
5.	Zunaira	23	MSC.IT	Student
6.	Uswa	21	BS. Nutrition	Student
7.	Nisha	20	BS.E-Commerce	Student
8.	Sana	24	BS. Physiotherapy	Student
9.	Durdana	23	BS.E-Commerce	Student



10.	<i>Kinza</i>	21	<i>BS.E-Commerce</i>	<i>Student</i>
11.	<i>Muqdas</i>	25	<i>BS.Nutrition</i>	<i>Working females</i>
12.	<i>Noor</i>	22	<i>BS. Accounting</i>	<i>Student</i>
13.	<i>Zaira</i>	23	<i>BBA</i>	<i>Student</i>
14.	<i>Iqra</i>	27	<i>B.COM</i>	<i>Student</i>
15.	<i>Fatima</i>	22	<i>B.A</i>	<i>Student</i>

Awareness of Cybercrime

The analysis of the thematic study on the collected data unraveling the multiple facets of understanding about cybercrime on the part of females who had not yet experienced victimization was quite revealing. The first theme emerged as Surface-Level Awareness. It posited that participants are generally aware of the term "cybercrime," however limited to identifying commonly recognized threats such as hacking, online harassment, identity theft, and social media scams. Most of this awareness came from social media channels, news outlets broadcasting reports on cybercrime, or word-of-mouth, not from any formal education or training. The analysis also highlighted "Perceived Distance" with regard to how close or far the participants feel cyber crime is likely to occur; it happens to someone else and that someone else is more of an online public citizen towards it. All of these allow an illusory sense of safety that then accounts for the difference between awareness and preparedness. As a whole, these findings underscore the need for more targeted cyber awareness initiatives that go beyond general knowledge and equip females with the skills and confidence to recognize, prevent, and respond to cyber threats effectively.

Awareness of Cybercrime is a major theme that emerged from the study. When participants were asked to reveal their understanding of and sources of information on cybercrime,



they expressed a variety of opinions. Most could readily define cyber crime as "crimes associated with or happening to computers," with several others indicating hacking was one of the better-known examples of cyber crime. Amina suggest about hacking, a 26-year-old working female, expressed her understanding of this threat in relatable terms.

I haven't experienced it myself, but I know hacking is real, like, people can break into your accounts and misuse your pictures or messages. That's why I don't share anything personal on my Facebook.

Amina's comments reflect the broader theme of surface-level awareness, where the recognition of Threats like hacking are present, yet largely informed by secondhand knowledge rather than Technical understanding or direct experience, her cautious approach to online activity also highlights A sense of preventive behavior, shaped more by fear and social influence than by structured Awareness or digital literacy training through narratives like Amina's, the study uncovers How young females are navigating their online presence with vigilance, despite a lack of In-depth understanding of cyber risks.

While Nimra described cybercrime as; I just know that cybercrime is something bad that happens on the internet. Researchers need to be careful; that's all researchers know. Nimra's statement illustrates the presence of broad awareness without depth, a common pattern among participants who had no direct experience with cybercrime. Her knowledge, while genuine, is based more on social narratives and cautionary tales rather than formal education or technological familiarity. This theme emphasizes the gap between awareness and empowerment, suggesting that while participants like Nimra



are alert to the risks, they often lack detailed knowledge of how cybercrime operates or how to respond effectively if targeted. Zunaira, a 23-year-old university student enrolled in an IT program, demonstrated a more informed perspective.

She explained, in our IT (Information Technology) classes, researchers studied topics like data protection, phishing, and how hackers work. It made me realize that cybercrime is not just about someone stealing your pictures; it can be much more serious, like identity theft or stealing money from your accounts.

Zunaira's comments represent the theme of informed awareness through academic exposure, which was less common among participants but impactful when present. Her deeper understanding of cybercrime and its various forms reflects the role that formal education can play, equipping young women with practical knowledge and digital resilience. Unlike many others who relied solely on social media or peer stories, Zunaira's awareness was grounded in structured learning, giving her a clearer sense of both the risk and the appropriate responses in the digital world. This was sounded by others who cited their university education as the primary source of awareness. However, some participants also mentioned learning about cybercrime through media, social media, or personal and family experiences.

Sana explained, a 24-year-old student, who described how she stays informed about cyber threats. She follow a few journalists and pages that post updates about these cases, so that's how I learn what's happening. Sana's account illustrates the theme of awareness through digital news exposure, where platforms like Twitter serve as informal yet impactful sources of real-time



information. Her comments reflect a growing trend where young women rely on social media not just for connection but for staying informed about safety concerns. While this form of awareness increases vigilance, it also tends to be emotionally charged and case-based, lacking the consistency or structure that formal education might provide. Still, Sana's experience shows that digital platforms can play a powerful role in spreading awareness and influencing online behavior among women. When it came to the participants' self-perceived knowledge of cybercrime, most expressed confidence in their understanding, stating they knew how cybercrime occurs and how to protect themselves. Usma remarked; a 21-year-old postgraduate student reflected this perspective in a clear and assertive manner.

*Yes, I have sufficiently
knowledge about how
cybercrime works. I've read
articles, attended webinars, and
I try to stay updated. I know
about things like phishing
emails, financial fraud, and even
cyber-stalking.*

So, I do take some precautions. Her statement highlights the theme of proactive digital literacy, where awareness is not only present but actively maintained through diverse information sources. Unlike others whose understanding was shaped by fear or secondhand experiences, Usma demonstrated a structured and confident grasp of cybercrime, reflecting both awareness and preparedness. Her engagement with educational resources suggests a growing shift toward



informed digital citizen ship among young women who actively seek to protect themselves in the online environment

While others, like Kinza: a 21-year-old undergraduate student openly acknowledged this in her response.

She expressed, I know the basics, but I could learn more. I've heard about cybercrime like online blackmailing or fake accounts, but Researcher don t really know what to do if something like that happens to me

Kinza's statement reflects a realistic and honest self-assessment, highlighting the theme of incomplete understanding and openness to growth. While she possesses a foundational awareness of cyber threats, her uncertainty about protective actions and legal recourse reveals a broader issue among participants awareness without empowerment. Her desire for further information suggests a potential area for targeted educational interventions that not only increase awareness but also build confidence and capability in responding to digital threats.

Despite this confidence, many participants only discussed general protective measures, such as using strong passwords or being cautious about sharing personal information online.

With Noor noting, a 22-year-old college student shared her perspective on cyber safety practices.

I haven't taken many additional steps, but I know the importance of a strong password.

Noor's response reflects a common pattern among participants who are aware of certain protective measures but have not fully implemented a broader range of cybersecurity practices. Her



awareness of password strength indicates a basic level of understanding, likely influenced by general digital use and common advice. However, the lack of further action points to a theme of limited engagement, where knowledge exists in theory but is not fully translated into behavior. Noor's response suggests that while young women may recognize certain safety tips, there remains a need for more hands-on guidance to transform awareness into consistent, protective habits online. While Hareem stated as; a 22-year-old university student expressed a strong awareness of this issue.

Sharing personal information on the internet is severe for females because it increases the chance of being more vulnerable

Hareem's reflection highlights the theme of gendered digital risk perception, where the act of simply existing online is often seen through a lens of caution and potential threat. Her statement demonstrates an acute understanding of how personal data can be exploited particularly in the context of cyber harassment and blackmail which many participants feared. This awareness shaped her own online behavior, leading her to limit what she posts and to be selective about who has access to her content. Hareem's perspective reinforces the finding that, for many women, cybercrime awareness is closely tied to concerns about privacy, dignity, and safety.

Naimal shared; a 20-year-old graduate student shared how her growing concern about online threats led her to take specific steps to protect herself.

I started looking into ways to stay safer online. I learned



*about two-step
verification,
making stronger
passwords, and
checking privacy
settings
regularly. It
gives me some
peace of mind.*

Naimal's experience reflects the theme of self-initiated digital empowerment, where awareness goes beyond theoretical knowledge and results in practical, protective actions. Her approach illustrates a shift from passive caution to active prevention, motivated by both a desire for safety and a sense of responsibility over her digital presence. This narrative highlight show, for some participants, exposure to cybercrime awareness even without direct victimization can trigger meaningful behavior change and foster a more resilient online identity

In summary, the participants differed in the degree to which they were aware of cyber crime and this was largely determined by their education, digital habits, and sources of information. Most had some knowledge regarding common cyber threats like hacking, fake accounts, and online blackmail, which they learned mostly through social media platforms, news stories, or from their peers. Sana for example, stated that she always kept herself updated through Twitter, while Nimra remembered general cyber issues but had to admit that her knowledge was limited. In the same trend, Zunaira was empowered to bring an



educated opinion because of her attending formal IT classes, showing how instituted education could stretch awareness. Similarly, Naimal made her own initiation of taking safety measures against the Internet by learning on two-step verification and stronger passwords. Kinza and Noor, on the other hand, echo a shallow understanding of the importance of cyber safety without much appreciation of the deeper facets or actions of it. Amina and Hareem fall in participants who put their emphasis on the amount of personal information one shares on the Internet regarding the risks for females, thus placing it in gendered perspectives on cyber awareness. Overall, none of the respondents has any personal experience with cybercrime; awareness rather ranges from minimal to moderately informed, with a collective understanding that such threats are very real and must be dealt with at all. These findings emphasize the need for a more targeted and practical awareness of cybercrime, particularly with programs that empower women.

Perceptions of Cybercrime

The theme of Perceptions of Cybercrime was focused on how participants viewed cybercrime severity and their personal risk perceptions. The pattern that was quite clear was that while the participants acknowledged cybercrime as an issue for women, their perceptions of personal vulnerability differed quite widely. Most of the participants agreed with the fact that women are most vulnerable in certain types of cybercrimes, including identity theft or online harassment, blackmailing, or scams. Nisha; a 20-year-old university student articulated this view clearly when she stated,

Females are more likely to be targeted



*because of online harassment or phishing
scams.*

Her perception reflects a widespread concern among female participants that their gender makes them more susceptible to certain types of cybercrime. This belief often stemmed from observed trends on social media, news stories, or incidents involving peers.

Nisha's comment highlights the theme of Perceived digital exposure, where being a woman in the online world is seen as inherently riskier. Such perceptions not only influence how participants interpret cyber threats but also affect their online behavior, often leading them to adopt more cautious and restricted digital practices in order to avoid becoming potential targets. However, there was a notable difference in how participants viewed their own risk. While some acknowledged a general sense of vulnerability, others,

Like Nimra; believed they were not at risk, a 23-year-old Student reflected this mindset in her response.

*I don't think I would be
targeted because I'm
careful with what I
share.*

Nimra's perception suggests a belief that responsible digital behavior can significantly reduce the risk of cyber threats. This theme of confidence in personal caution was evident in a few participants who associated low visibility and controlled sharing with lower vulnerability. While this reflects a level of awareness and digital discipline, it also hints at a potential underestimation of how sophisticated or unpredictable cybercrime can be. Nimra's narrative



illustrates how some females, despite acknowledging cybercrime as a real issue, may not fully perceive themselves as potential victims due to their controlled online presence.

Emotional reactions to the thought of being targeted by cybercriminals were mixed. Some participants showed a degree of concern, expressing unease, anxiety, stressed, depression, at the possibility of being victimized. Iqra mentioned; a 27-year-old student expressed this apprehension stating.

*It does worry me, especially with the rise of
online scams.*

Her comment reflects the theme of heightened digital anxiety, where awareness of real-world cases fuels a sense of unease; even among those who have not been directly affected Iqra's perception illustrates how the visibility of cybercrime in media and social networks contributes to a constant undercurrent of fear and caution, especially for females navigating online spaces. Her concern is not rooted in personal experience but in an evolving digital landscape where the threat appears increasingly close and unpredictable. This theme reveals how cybercrime is not only understood as a technical issue, but also felt as an emotional and psychological concern by users who feel they must constantly remain on guard

In contrast other participants, like Amina seemed in different way a 26-year-old undergraduate Student reflected this mindset in her response.

*She remarked, it does not bother me if I were to be
targeted*



Her statement reveals a theme of minimized personal concern where the perceived seriousness of cybercrime is downplayed or not fully internalized. This sense of indifference may stem from a belief that the likelihood of being targeted is low or from a coping mechanism that distances the individual from the emotional weight of digital threats. In Amina's case, this detachment could also suggest a lack of first hand exposure to cyber incidents or a limited understanding of their potential impact. Her perspective contrasts sharply with participants who expressed fear or took active precautions, illustrating a diverse range of perceptions from hyper-vigilance to passive acceptance among females who have not personally experienced victimization. Amina's indifference underscores the importance of tailored awareness efforts, as not all individuals are equally motivated to engage in self-protective behaviors unless they perceive a personal threat.

This indicates a broad range of emotional responses to cybercrime, with some participants perceiving it as a serious threat and others downplaying the risks. Furthermore, many participants expressed ambivalence toward sharing personal information online. Some indicated that they take precautions when sharing details, others felt comfortable with it, particularly when the information was shared for important work.

As Hareem a 22-year-old university student articulated this balanced approach in her response.

I used for work-related purposes, I shared only my work related details, but I'm cautious in other situations like sharing personal details

Hareem's perspective reflects the theme of conditional caution,



where the decision to share information is influenced by the perceived legitimacy or necessity of the context. Her willingness to disclose details in professional settings suggests a level of trust in structured, goal-oriented environment such as job applications, academic networks, or official communications while maintaining a guarded approach in more casual or unknown digital spaces. This selective behavior indicates a growing digital discernment among some female users, who are learning to navigate online risks without completely withdrawing from online engagement. Hareem's narrative illustrates a thoughtful balance between functionality and safety, acknowledging the importance of maintaining an online presence while also recognizing the potential for misuse. Her perception highlights that awareness of cybercrime does not always translate into fear or avoidance, but rather into a more strategic and context-aware digital behavior, especially among those who use the internet for career advancement or academic purposes.

Overall, general perceptions of cybercrime among participants were diverse and multifaceted in how they constructed an opinion through their beliefs or experiences and exposure to digital activities. For some, like Nisha and Iqra, this raised the genuine anxieties regarding increasing threats of online harassment and fraud, especially against women; while for one, it was Nimra; her persona was safe enough as she followed very careful behaviors while Online. For Amina, there was a hint of not-much-feeling doubt being targeted or perhaps not much relevance perceived, as for Hareem, she had a more balanced stand, that is willing to share information for occupational purposes, but careful in personal context. Naimal's pro-activity



to learn and Uswa's self-assurance indicated strong control and awareness, while Kinza accepted limited knowledge and willingness to improve. Some like Sana got updates from social media news, while Zunaira availed formal education in IT, and Noor understood the need for basic security measures despite doing little to act. Overall, it reveals that all participants realized cyber crime is present but defines personal susceptibility and indifference well apart. Much of this had to do with the digital habits and the sources from which they drew awareness, and up to what level assessed personally they attached relevance or importance to these threats. The differences in responses indicate the need for individualized cyber education based on the emotional attitudes and behavioral tendencies toward online safety.

Responses to Cybercrime

The third theme, Hypothetical Responses to Cybercrime, sought to explore how participants would respond if they were to become victims of cybercrime. Responses varied but there were common threads regarding reporting behavior, desired support, and the confidence participants had in handling such situations. A majority of participants indicated that they would report a cybercrime if they fell victim to one. However, their choices of who to report to varied. Some participants preferred formal institutions such as the Federal Investigation Agency (FIA), while others would turn to tech companies or local authorities. For instance Durdana; a 23-year-old student, who demonstrated a clear awareness of legal recourse. Her response highlights the theme of formal institutional trust, showing that she not only recognizes the seriousness of cyber threats but also knows where to turn for legal help. Durdana's mention of the



Federal Investigation Agency (FIA) indicates an understanding of available cybercrime reporting channels in Pakistan, a point not commonly raised by other participants. Her conditional phrase if it were something serious also reflects a threshold-based approach, where only certain types of incidents are seen as worthy of official intervention. This suggests that while awareness of reporting mechanisms exists, decisions to act may depend on how participants interpret the severity or impact of the situation. Durdana's narrative underscores an important insight: some women are prepared to seek formal help, but only when the threat crosses a certain personal boundary. This reflects a need to strengthen not only awareness of legal rights but also confidence in using those channels even for what may initially seem like minor Cyber incidents. While Naimal mentioned; *a 20-year-old graduate student illustrated this targeted approach in her response.*

*I would contact to my bank if it was related to
financial fraud*

Naimal's statement reflects a clear and action-oriented mindset, where she not only recognizes the risk of cybercrime but also understands the importance of contacting the appropriate authority based on the situation. Her response highlights the theme of specific institutional awareness, particularly in relation to financial security a growing area of concern in the digital age. Unlike more general or emotionally driven reactions, Naimal's planned response suggests preparedness and confidence in navigating such incidents. It also implies a level of digital maturity, where she is not only aware of the threat but also familiar with the correct response channels, such as



contacting her bank to secure accounts and prevent further loss. Her perspective stands in contrast to participants who may rely solely on informal networks or hesitate to act at all. Naimal's response underscores the importance of equipping individuals especially women with not only knowledge of cyber threats but also the practical steps and institutional contacts necessary to respond swiftly and effectively when incidents occur. Confidence in responding to a cybercrime attack was generally high among participants.

Many felt prepared to handle such an event, with Uswa asserting a 21-year-old postgraduate student exemplified this mindset with her assertive response.

I feel very confident in reporting and seeking help if needed.

Uswa's comment reflects the theme of empowered digital citizenship, where awareness is not just passive knowledge but is backed by the willingness and self-assurance to engage with formal systems for support. Her confidence likely stems from a combination of factors, including prior learning, exposure to reliable information, and a clear understanding of her rights and the available reporting mechanisms. Unlike participants who expressed hesitation or uncertainty, Uswa presents a proactive stance demonstrating that some young women not only recognize cyber threats but also trust in legal and institutional structures to respond effectively. This level of assurance is vital in changing the broader narrative around cybercrime, where victims especially women often remain silent due to fear, stigma, or lack of knowledge. Uswa's narrative



represents a positive shift toward resilience and agency, suggesting that when individuals are equipped with the right tools, information, and mindset, they are more likely to respond swiftly and assertively if victimized. Her perspective emphasizes the importance of strengthening digital education programs that not only increase awareness but also build confidence in seeking help and using legal protections when necessary. This confidence, however, did not necessarily translate into practical preparedness. When asked if they had considered how they would react to identity theft or scams, many participants admitted that they had not thought about it in depth.

Muqdas remarked; a 25-year-old working female, honestly admitted, *“I haven’t really considered what I would do if I were scammed”*. Her response highlights a common theme of unpreparedness and hesitation, especially among those who have never faced such situations before. Muqdas’s words reflect how many people despite being aware that cybercrime exists haven’t taken the time to think about what steps they would take if it actually happened to them. This could be due to a false sense of safety, lack of awareness about reporting options, or simply not expecting to become a target. Her response shows that for some, cybercrime still feels like a distant issue rather than a real personal threat. This kind of uncertainty suggests a need for more practical education not just about what cybercrime is, but about what to do when it happens. People like Muqdas would benefit from clear, step-by-step information on how to report a scam, who to contact, and what actions to take immediately. Her honest answer serves as a reminder that knowing about cybercrime isn’t enough



people also need to feel prepared and supported to act if they ever find themselves in such a situation

Zaira emphasized; a 23-year-old university student shared her thoughts honestly

*She said I would like to have
more information on what steps
to take and whom to contact if
something happens*

Her words highlight a common feeling among many young women they want to protect themselves, but they don't always know how. Zaira's response reflects the theme of information gaps in response readiness. She isn't unaware or careless; in fact, she's thoughtful and cautious. But like many others, she lacks clear, accessible guidance on what to do in the event of cybercrime. This includes knowing the proper reporting channels, such as government agencies, legal authorities, or support services. Her comment shows a real need for awareness campaigns and education programs that focus not just on what cybercrime is, but on how to respond in a calm, effective way. Zaira's openness to learning also shows that young women are willing to take action they just need someone to show them the way. Her voice represents many others who feel the same: concerned, alert, but still searching for direction. Confidence vs. Experience Participants often claimed they were "very confident" in handling a cybercrime situation, but this confidence was not always backed by clear plans.

Her answer wasn't overly detailed or planned out, but it reflected a kind of quiet confidence a belief that if something went wrong, she'd figure it out in the moment. Hareem hasn't



faced anything like this before, and because of that, she hasn't really prepared for it. Still, there was a sense of self-trust in her words. She seemed to believe that she'd be able to handle the situation somehow, even if she didn't know exactly how yet. Her response is something many people can relate to: I don't always plan ahead for things we've never experienced, but Researcher hopes our instincts will guide us when the time comes. Her words also show a small gap like many others, she might benefit from a little more information, just in case. But at the same time, her confidence is strength. Hareem's story reminds us that's sometimes people aren't fully prepared, but that doesn't mean they're helpless they just need the right support and tools to turn that confidence into action when *It really counts*. This reflects a confidence-preparedness gap many participants had not considered detailed response strategies. Desired Resources and Support: A recurring suggestion was the need for public awareness campaigns, guidelines, and university-level workshops.

Fatima noted; a 22-year-old student shared a thoughtful suggestion when talking about how she would respond if she ever faced cybercrime. Her words didn't come from fear, but from a place of wanting to be prepared. She admitted that while she's heard about online scams and harassment, she wouldn't know exactly what to do if something happened to her. It wasn't that she didn't care she simply hadn't been taught what to do. That's why her idea made so much sense: a simple, short session at the university could make a big difference. Not long lectures or complicated courses just clear, practical advice on what to do, who to contact, and how to protect yourself. Fatima's comment stood out because it wasn't just about her



own response. She was thinking about all students. She knew that many of her friends also felt unsure about how to handle cyber threats. In her view, giving young people the right tools before something happens is better than expecting them to figure it out alone afterward. Her suggestion shows that students are ready to learn they just need the chance and the right support.

Many also wished for easier access to information from agencies like FIA, saying Nisha “Nisha leaned back slightly, thinking for a moment before she spoke. Then she said with calm honesty, *“Help from FIA would be good. They should have a helpline or a simple website”* It wasn’t just a passing thought it was something she clearly felt needed attention. She hadn’t experienced cybercrime herself, but the possibility was always there. What bothered her most wasn’t just the threat, but the lack of easy help. Nisha believed that even if someone wanted to Report something, they might not know how. She imagined how helpful it would be if there were a clear helpline or a user-friendly website, something simple no complicated forms or confusing links. Just a place where people, especially women, could quickly get guidance or report a problem without fear or confusion her response showed that she wasn’t just thinking about herself, but about others too people who might panic or freeze up if something bad happened Online. For nisha, it wasn’t about just being aware; it was about having a system that works a support system that feels real, reachable, and ready. Her words were a reminder that awareness alone isn’t enough. Without easy access to help, even the most alert person can feel stuck. Nisha’s voice adds something important



to the conversation: prevention is good, but quick and simple support matters just as much.

The responses by the participants showed a great divergence of attitudes and preparedness toward dealing with cybercrimes. While some contestants were confident and had a clear strategy, others admitted that they have not really thought about it. A few, like Uswa and Durdana, indicated they would take formal action-reporting incidents to authorities like the FIA or contacting the right institutions if something went wrong. Naimal, for example, said she would call her bank if it were financial fraud and reflects a practical and informed approach. But confess against those lines are Muqdas and Hareem-they have not really thought about anything they would do in case something earthly happens to them.

In fact, most of the responses seem to mirror a general problem-not concern but lack in preparation along with less clear guidance. Meanwhile, participants like Zaira and Fatima expressed more robust needs for support systems, e.g., short sessions in training at universities or simple instructions on basis for seeking assistance. Amina has also expressed the view that such systems should be made accessible; that the FIA should provide a clear helpline or a user- friendly website for quick action.

Overall, all these participants showed some tendency as victims of cybercrime to respond when it happens to them, but this response was fully varied. Some were confident, some were doubtful, and others were quite uncertain about support. Most significant is that awareness alone is not enough: there



is a real gap between knowledge and action, and actionist education on

How and what to do, whom to contact, and how to keep people safe from a possible cyber threat in the future was needed. Thus, reading that gap would ensure that even more women are empowered not just to identify cybercrime but also to take action against it-and without hesitation.

5. DISCUSSION AND SUMMARY

5.1 Summary of Findings: Awareness, Perception, and Hypothetical Response to Cybercrime

Conversations with the study participants revealed various opinions and ranges of feelings about cybercrime. Nobody had been victimized; rather, each person holds certain perspectives, beliefs, and ideas regarding how they would react should it ever happen to them.

Most of those interviewed expressed that they were aware of mainstream cybercrimes such as hacking, blackmail, fake accounts or scams. Some learned more through classes on cyber safety and IT in the university while others raised their awareness by following real-life cases over Twitter or other social media. Participants such as Naimal took matters into their own hands to learn how to generate strong passwords and enable two-step verification. However, a few admitted they only knew basics, and it would benefit them to learn more about the subject. Generally speaking, there was some level of awareness among participants about some aspects of cybercrime, yet it was often rather shallow in content or technicality. Many knew the risks were present but were not aware of how to protect them on a deeper level.



When describing their perception, participants were divided in opinion. Nisha and Iqra held the view that women are at greater risk of being targeted on the internet, particularly in cases of harassment and scams. Other participants argued that they were not personally at risk because they consciously limited what they shared online. Some was quite apathetic and said she wouldn't highly care if targeted, while few imagined herself in different contexts: Share freely in one, be careful in another. Some exhibited some anxiousness but were willing to learn. These diverse perspectives illustrate how women's ideas about online safety are mediated by personal experience, belief structures, and digital habits. Some find the turf familiar and secure, while others feel unsure and vulnerable. When the expected diverse responses to cybercrime came, equally diverse answers were forthcoming. Few participants firmly asserted that they would lodge a report with the authorities, perhaps even the FIA, if required. Naimal declared she would rush straight to her bank in the event of financial fraud, implying that some women know the prescribed point of authority based on the alleged issue. Participants also did not think of any real-way interventions, but felt that there would somehow be a way out for them. suggested more useful ways; wanted more information on what steps to take, while Fatima proposed that universities offer short trainings in digital safety. Some also mentioned that a helpline would help mobilize people fast and a simple FIA website as a means of action. These voices point toward the fact that while some women know how to respond, many still feel uncertain and lack insight into how to go about it, thus calling for improved support systems and clear directives.



Table 2: Thematic Analysis Summary

Main Theme	Sub-Theme	Description	Illustrative Quotes (Participant)
1. Awareness of Cybercrime	Surface-Level Awareness	General knowledge from social media, peer talk, or news; lacking depth or formal training	“Researcher just know that cybercrime is something bad...” – Nimra
	Informed Awareness (Academic Exposure)	Understanding gained through formal IT or E-commerce education	“In our IT classes, Researcher studied topics like data protection...” – Zunaira
	Awareness via Digital News/Social Media	Learned through platforms like Twitter, digital journalism	“Researcher come across cybercrime cases on Twitter...” – Sana
	Proactive Digital Literacy	Participants read articles, attended webinars, actively engaged in self-learning	“Researcher tries to stay updated. Researcher know about phishing, fraud...” – Uswa
	Incomplete Understanding & Desire to Learn	Participants knew the basics but admitted they needed more information	“Researcher knows the basics, but could learn more.” – Kinza
	Gendered Risk Awareness	Awareness of how online behavior may increase vulnerability as females	“Even small details can be misused by someone with bad intentions.” – Hareem
	Perceived Digital Vulnerability	Belief that females are more at risk due to online harassment, scams, identity theft	“Females are more likely to be targeted...” – Nisha
2. Perceptions of Cybercrime	Confidence in Careful Behavior	Some believed their cautiousness makes them less vulnerable	“Researcher don’t think Researcher would be targeted; I’m careful...” – Nimra
	Digital Anxiety	Concern, anxiety, or fear about becoming a victim despite not experiencing it directly	“It does worry me, especially with the rise of online scams.” – Iqra



Main Theme	Sub-Theme	Description	Illustrative Quotes (Participant)
3. Likely Responses to Cybercrime	Emotional Detachment	Downplaying seriousness of cybercrime or lacking concern	"It does not bother me if Researcher were to be targeted." – Amina
	Conditional Caution	Willing to share personal info when necessary (e.g., academic/job context), but careful otherwise	"For work-related purposes, I don't mind sharing details." – Hareem
	Formal Institutional Trust	Participants expressed willingness to report to official bodies like FIA	"Researcher would report it to the FIA..." – Durdana
	Targeted Reporting (Financial Institutions)	Preferred contacting specific institutions for certain crimes (e.g., bank for financial fraud)	"Researcher would contact his bank..." – Naimal
	Empowered Digital Citizenship	Confidence in reporting, engaging legal resources, self-assurance	"Researcher feel very confident in reporting..." – Uswa
	Unpreparedness	Admitted lack of clear action plans despite being aware of cybercrime	"Researcher haven't really considered what Researcher would do..." – Muqdas
	Need for Institutional Support	Suggested training, workshops, simple reporting platform	"It would help if universities gave a short training..." – Fatima
	Confidence vs. Actual Readiness Gap	Expressed self-confidence but lacked structured plans or knowledge	"I've never thought about what I'd do, but I'd manage." – Hareem

5.2 Discussion

The results indicate that most of the respondents have a general inclination to report cybercrime when victimized; but rather as the case with preparedness and knowledge of available mechanisms, it also varies. Many respondents trust formal



institutions, primarily for the reason of reporting such a serious incident to the Federal Investigation Agency (FIA): for instance, she would head towards FIA for reporting, assuming the case of cybercrime is “*something serious*”; this means that institutional trust does exist but only conditionally or very dependent on the seriousness of the offense.

Another group identified reported targeted reporting, particularly for crimes involving money. One participant said she would contact her bank if fraud was committed; indicating a situation-based approach to reporting according to the understanding of what type of cyber crime has taken place. Some of the respondents display empowered digital citizenship where their attitude towards reporting cyber threats is that of self-confidence and an active posture. For example, 1 participant revealed that she was quite sure about reporting and seeking assistance, as she felt “very confident” with the situation. Such levels of confidence are promising and indicate that educational exposure and self-generated learning have significant roles in empowering digital resilience.

As much as there are still signs of awareness and readiness to report, there was indeed another breaking theme even more inconsistent; unpreparedness. In fact, a lot of the respondents stated that they were aware of what cybercrime was but not how it would happen to them and did not have any ideas about what they would do about it. Other participant, proved her unpreparedness because she admitted that she had not really thought through the steps she would take should she be scammed. So, this speaks of the gap between awareness and preparedness in theoretical terms and preparedness in practical



terms, which would leave individuals vulnerable in real-life cybercrime scenarios.

In addition, it was highlighted by many participants about the need for institutional support. Structured training programs that would provide awareness campaigns on such cases in clear reporting procedures were necessary. One participant suggested that universities could hold short practical workshops on digital safety, particularly stressing the need for education that is accessible and not abstract.

To sum up, the analysis showed that both confidence and actual readiness gap. Some participants, were self-confident when it comes to managing cyber incidents, yet on the other hand, she admitted what she would have done was not much in their mind. This disconnect suggests that while confidence is present, it is not always based on actionable knowledge or plans. Thus, findings point to the fact that more young women are knowing about cyber threats then wishing to think and act on them, but there are clear differences among them in terms of actual preparedness. This calls for targeted educational interventions aimed at strengthening awareness while putting in place practical skills for action as supported by institutions, such as universities or national cybercrime units.

5.3 Conclusion

The study examined the perceptions, awareness, and probable responses of young women but not personally affected by cybercrime, and understood that with the advent of the digital age, they were becoming more and more threatened in this regard. The thematic analysis of the narratives provided by participants indicates the general acknowledgment of



cybercrime as a serious and rising problem; however, it is evident that varying depths of knowledge or awareness exist. While most said that their knowledge is perhaps surface when it comes to cyber threats like hacking, identity theft, blackmail, and scams, that information was predominantly gained through social media and talking to peer groups or digital news platforms with few exceptions of those few. Only a few respondents had informed awareness through learning in more formal IT-related disciplines. Hence, there is an urgent need to include structured education on cybercrime in the academic curriculum and informal learning spaces.

Nevertheless, perceptions of vulnerability were highly gendered. Most participants thought being female increased one's risk of victimization using public digital platforms. While some displayed anxiety in the digital world, others seemed emotionally detached or held the opinion that their carefulness reduced risks. These differences in perceptions also determined the participants' online habits, where some avoided sharing too many personal details online while some shared selectively based on the context.

Participants would give mixed responses regarding the likely reactions to cybercrime. While some students have confidence and will report to the formal institution such as FIA or bank in case of financial fraud, others depicted the gap between confident thinking and being ready, and they admitted having never thought of how to respond in the incident of such happening. Most participants expressed a lack of such reporting mechanisms and essentially no user-friendly support systems against such abuse. There was a call for increased institutional



support, particularly through workshops, training, or simplified reporting procedures.

Therefore, first of all, young women may be more aware of cyber crime, but the depth of the awareness usually does not lead to full action. The perceptions are gendered, emotive responses varied and confidence did not always translate to preparedness. Such findings highlight the urgent need for targeted, practical and inclusive programs on cyber education - initiatives that would go beyond the usual dangers usually warned against and empower women to handle the tools, knowledge and confidence to protect them and act in digital space.

5.4 Limitations

- Most of the participants were young women in an academic environment and probably do not reflect a range of other age groups, different culture backgrounds, or rurality among females.
- Participants had not been victims of cybercrime, making perceptions instead of assumptions the measure of the study, rather than actual behavior in response to victimization.
- Findings are typically based on self-reported narratives, which memory bias, social desirability bias, or emotional framing would affect their authenticity and reliability in the respondents' said findings.
- The research had been limited to a sample of respondents from a specific geographical location (most probably urban Pakistan) and thus may be limiting the findings from being generalizable to other cultural or other regional contexts.



- Only basic cyber threats such as hacking, fake accounts, or blackmailing were discussed by participants, while more intricate or unrecognizable cybercrimes, e.g., spyware and ransomware, were not reviewed in detail.
- The study has adopted a qualitative-only methodology, thus limiting the findings from statistical generalization. Mixed methods approach might have provided wider validation of findings.
- This research examined female perspectives without balancing or enriching the opinions of law enforcement agencies, cybersecurity experts, or educators.

5.5 Recommendations

- Mandatory courses and workshops on digital safety need to be compulsorily included in general knowledge imparting to all the universities and colleges. Simple, user-friendly modules could provide basic awareness of the day-to-day e-safety issues to protect young women, with a major focus on issues like phishing, identity protection, how to report breaches, and data privacy thereof.
- As a fighting-arm against cybercrimes, students should become the end-point users trained to watch out for things, which could retaliate on giving verified information, and aid in setting up an all inclusive support system within campuses or city blocks.
- Training sessions by FIA officers or lawyers specialized in cybersecurity will clear the air with regard to legal rights, processes for reporting, and the like in cybercrime cases.
- Women from rural areas, different age groups and behavioral groups like nurse or housewife should be inducted in reflection on future efforts and questions:



- whether the inclusion of such diverse women would ensure inclusive policymaking and resource development.
- Collaboration between major social media platforms and regulators (e.g. Facebook, X/Twitter, and Instagram) should result in the development of safety education features within the platforms, such as in-app reporting facilities.
 - A special kind of digital help desk should be maintained at the university level to guide the students with problems regarding reporting, privacy settings, password recovery, and threats online, providing real-time support and advice on the matter.

REFERENCES

- Abu-Bakr, A. M. (2020). A study on cybersecurity awareness among students in Yobe state university, Nigeria: A quantitative approach. *Www.academia.edu*, 11(5), 41–49. https://www.academia.edu/92333835/A_Study_on_Cybersecurity_Awareness_Among_Students_in_Yobe_State_University_Nigeria_A_Quantitative_Approach
- Aleem, Y. (2022). Cybercrimes against women in Pakistan: Feminist narratives of resistance, resilience & coping strategies. *ResearchGate*. https://www.researchgate.net/publication/361445811_Cybercrimes_Against_Women_in_Pakistan_Feminist_Narratives_of_Resistance_Resilience_Coping_Strategies
- Alnajim, A. M., Habib, S., Islam, M., AlRawashdeh, H. S., & Wasim, M. (2023). Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches. *Symmetry*, 15(12), 2175. <https://doi.org/10.3390/sym15122175>
- Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437–443. <https://doi.org/10.1016/j.chb.2016.12.040>



- Artfield, M. (2015). Towards a cyber victim logy: Cyber bullying, routine activities theory, and the anti-sociality of social media. *Canadian Journal of Communication*, 40(3). <https://doi.org/10.22230/cjc.2015v40n3a2863>
- Aslam, S. B., Malik, M. A., & Khan, M. A. (2023). Gender and cyber communication: A systematic literature review of challenges faced by women in Pakistan. *Global Language Review*, 8(1), 174–183. [https://doi.org/10.31703/glr.2023\(viii-i\).17](https://doi.org/10.31703/glr.2023(viii-i).17)
- Aslam, Ö. Aktuğ, S. S., Okay, M. O., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6), 1–42. <https://doi.org/10.3390/electronics12061333>
- Bada, M., & Nurse, J. R. C. (2020). The social and psychological impact of cyber attacks. *Emerging Cyber Threats and Cognitive Vulnerabilities*, 73–92. <https://doi.org/10.1016/b978-0-12-816203-3.00004-6>
- Balaji, M., Mandhare, K., Nikhare, K., Shah, A. K., Kanhere, P., Panse, S., Santre, M., Vijayakumar, L., Phillips, M. R., Pathare, S., Patel, V., Czabanowska, K., & Krafft, T. (2023). Why young people attempt suicide in India: A qualitative study of vulnerability to action. *SSM - Mental Health*, 3, 100216. <https://doi.org/10.1016/j.ssmmh.2023.100216>
- Baraković, S., & Husić, J. B. (2022). Cyber hygiene knowledge, awareness, and behavioral practices of university students. *Information Security Journal: A Global Perspective*, 32(3), 1–24. <https://doi.org/10.1080/19393555.2022.2088428>
- Basit, H., Sajjad, A., Sarwar, A., & Nooral, A. (2024). Cyber harassment helpline report. In N. Dad & S. Khan (Eds.), *Digital Rights Foundation* (pp. 4–46). Digital Rights Foundation. <https://digitalrightsfoundation.pk/wp-content/uploads/2024/04/DRFs-Cyber-Harassment-Helpline-Report-2023.pdf>
- Bhongale, Dr. J. K. (2021). Crime against women in cyber world. *SSRN Electronic Journal*, 1–16. <https://doi.org/10.2139/ssrn.3903959>
- Caeiro, D. (2024). A review on the application of lifestyle-routine activity theory in cyber criminology riya raj CA. *Scholars Publishers J Forensic Res Crime Stud* 2024 |, 9, 101.



- <https://www.jscholaronline.org/articles/JFRC/A-Review-on-the-Application-of-Lifestyle-Routine-Activity-Theory.pdf>
- Chaudhry, S. (2024). Cyber security threats in social media. In *ResearchGate*.
https://www.researchgate.net/publication/381106898_Cyber_Security_Threats_in_social_media
- Chaudhry, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. *Computer Science Review*, 50, 100592.
<https://doi.org/10.1016/j.cosrev.2023.100592>
- Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q., & GAO, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*, 10(1).
<https://doi.org/10.1057/s41599-023-01560-x>
- Com Digful. (2022). Understanding cybersecurity law and digital privacy: Melissa lukings arash habibi lashkari. *Scribd*.
<https://www.scribd.com/document/556565278/Future-of-Business-and-Finance-Melissa-Lukings-Arash-Habibi-Lashkari-Understanding-Cybersecurity-Law-and-Digital-Privacy-a-Common-Law-Perspectiv>
- Council of Europe. (2023). *Feminism and women's rights movements*. Gender Matters; Council of Europe.
<https://www.coe.int/en/web/gender-matters/feminism-and-women-s-rights-movements>
- Crane, C. (2022, February 16). *By the numbers: 50 cyber crime statistics for 2025*. Hashed out by the SSL Store™.
<https://www.thesslstore.com/blog/cyber-crime-statistics/>
- Dennis, M. (2019). Cybercrime | definition, statistics, & examples. In *Encyclopædia Britannica*.
<https://www.britannica.com/topic/cybercrime>
- Dwivedi, Y. K., Ismagilova, E., Hughes, D. L., & Carlson, J. (2021). Setting the future of digital and social media marketing research: Perspectives and research propositions. *International Journal of Information Management*, 59(1), 1–37. Science Direct.



- Garba, A. A., Siraj, M. M., Musa, M. A., & Othman, S. H. (2020). A study on cybersecurity awareness among students in Yobe: A quantitative approach. *ResearchGate*, 41–49. https://www.researchgate.net/publication/343600853_A_Study_on_Cybersecurity_Awareness_Among_Students_in_Yobe_A_Quantitative_Approach
- Griffiths, C. (2025, April 1). *The latest 2022 cyber crime statistics (updated December 2022) | AAG IT support*. AAG. <https://aag-it.com/the-latest-cyber-crime-statistics/>
- In, & Malik, S. (2022). Cyber security situation in Pakistan: A critical analysis. *Pal Arch S Journal of Archaeology of Egypt / Egyptology*, 19(01), 23–32. https://www.researchgate.net/publication/376232423_Cyber_Security_Situation_in_Pakistan_A_Critical_Analysis
- Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications*, 241(122697), 122697. <https://doi.org/10.1016/j.eswa.2023.122697>
- Jurgens, J., & Dal Cin, P. (2025). Global cybersecurity outlook 2025. In *World Economic Forum* (pp. 3–47). World Economic Forum. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf
- Kala, E. S. M. (2023). Critical role of cyber security in global economy. *Open Journal of Safety Science and Technology*, 13(4), 231–248. <https://doi.org/10.4236/ojsst.2023.134012>
- Kannathasan, B., & Murugan, D. K. R. (2015). Nature and impact of cybercrime against girls. *ResearchGate*, 1(8), 21–24. https://www.researchgate.net/publication/349173105_Nature_and_impact_of_cybercrime_against_girls
- Kaspersky. (2019, December 5). *Tips on how to protect yourself against cybercrime*. [Www.kaspersky.com. https://www.kaspersky.com/resource-center/threats/what-is-cybercrime](https://www.kaspersky.com/resource-center/threats/what-is-cybercrime)
- Khalid, H. M. B., Guriro, S., Lakho, M. K., & Shaikh, S. U. D. (2022). Cyber bullying awareness among students of universities in Sindh. *ResearchGate*, 19, 1–16. https://www.researchgate.net/publication/361736891_CYB



ER_BULLYING_AWARENESS_AMONG_STUDENTS_
OF_UNIVERSITIES_IN_SINDH

- Khan, Dr. I. A., Irshad, S., & Ud Din, H. S. J. (2025). Cyber harassment and online violence against women: a critical analysis of women protection law regime in Pakistan. *Journal of Law & Social Studies*, 7(1), 12–25. <https://doi.org/10.52279/jlss.07.01.1225>
- Khan, S. (2022). Cyber security challenges in Pakistan: An assessment. *ResearchGate*, 1(1), 78–89. https://www.researchgate.net/publication/360256123_Cyber_Security_Challenges_in_Pakistan_An_Assessment
- Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, 28(7), 509–520. <https://doi.org/10.1016/j.cose.2009.04.006>
- Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *JOURNAL of INTERNATIONAL STUDIES*, 17(2), 220–239. <https://doi.org/10.14254/2071-8330.2024/17-2/12>
- Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. *Energy Reports*, 7(7), 8176–8186. Science direct. <https://doi.org/10.1016/j.egy.2021.08.126>
- Madarie, R., Kranenbarg, M. W., & Poot, C. de. (2025). Cybersecurity expert perspectives on data thieves' actions in digital environments: Potential refinements for routine activity theory. *Deviant Behavior*, 1–19. <https://doi.org/10.1080/01639625.2025.2453440>
- Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity enterprises policies: A comparative study. *Sensors*, 22(2), 538. <https://doi.org/10.3390/s22020538>
- Nahar, H. L., & Emran, A. K. M. (2021). Applying routine activity theory to cyber victimization: A secondary analysis. *ResearchGate*, 3(3), 69–87. https://www.researchgate.net/publication/392322989_Applying_Routine_Activity_Theory_to_Cyber_Victimization_A_Secondary_Analysis



- Pandey, P., & Kapoor, A. (2025). Cybercrime in the digital era: Impacts, awareness, and strategic solutions for a secure future. *Sachetas*, 4(1), 32–37. <https://doi.org/10.55955/410004>
- Petrosyan, A. (2024, November 15). *Global cybercrime estimated cost 2028*. Statista. <https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide>
- Poulpunitha , D. S., Kalidasan , M., & Veeramani , P. (2020). Strategies to prevent and control of cybercrime against women and girls. *International Journal of Innovative Technology and Exploring Engineering*, 9(3), 609–612. <https://doi.org/10.35940/ijitee.k2408.019320>
- Qureshi, S. F., Abbasi, M., & Shahzad, M. (2020). Cyber harassment and women of Pakistan: Analysis of female victimization. *Journal of Business and Social Review in Emerging Economies*, 6(2). <https://doi.org/10.26710/jbsee.v6i2.1150>
- Rafaqat, S., Shabbir , T., & kumari, S. (2024). Feminist movement in Pakistan as a cybercrime act: Challenges and consequences . *Annals of Human and Social Sciences (AHSS)*, 5(3), 841–853. P-ISSN: 2790-6795. [https://doi.org/10.35484/ahss.2024\(5-III\)76](https://doi.org/10.35484/ahss.2024(5-III)76)
- Rasheed, A., Mishra, L. K., & Tiwari, G. K. (2024). Internet addiction among higher secondary and university students in India: A post-covid assessment. *Caspian Journal of Health Research*, 9(3), 135–142. <https://doi.org/10.32598/cjhr.9.3.486.2>
- Riaz, K. (2021, March 26). *Does PECA law empower women? - Centre for strategic and contemporary research*. Centre for Strategic and Contemporary Research. <https://cscr.pk/explore/themes/social-issues/does-peca-law-empower-women/>
- Saleem, H., Jan, J., & Areej, A. (2022). Cyber crimes trends in Pakistan: Analyzing the legal framework and enforcement challenges. *Deleted Journal*, 1(1), 10–22. <https://doi.org/10.62585/slpr.v1i1.21>
- Sentinel One. (2024, September 16). *Key cyber security statistics for 2024*. Sentinel One.



- <https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/>
- Shabbir, N., & Adnan, Dr. M. (2025). Cyber security: A growing challenge to Pakistan. *Annals of Human and Social Sciences (AHSS)*, 6(1), 372–384. [https://doi.org/10.35484/ahss.2025\(6-I](https://doi.org/10.35484/ahss.2025(6-I)
- Shahzad, M. (2023). Emerging cyber crimes in Pakistan: A case study of online fraud through digital microloan apps. *Global Digital & Print Media Review*, VI (II), 411–421. [https://doi.org/10.31703/gdpmr.2023\(vi-ii\).30](https://doi.org/10.31703/gdpmr.2023(vi-ii).30)
- Singh, A., & Singh, K. (2025, June 30). *Technology revolution gives cybercrime a boost: Cyber-attacks and cyber security*. ResearchGate. https://www.researchgate.net/publication/348923007_TECHNOLOGY_REVOLUTION_GIVES_CYBERCRIME_A_BOOST_CYBER-ATTACKS_AND_CYBER_SECURITY_1
- Tarar, M. G., Alvi, A. S., Aleem, Y., & Bajwa, A. (2021). *Cybercrimes against women in Pakistan: Feminist narratives of resistance, resilience & coping strategies*. Csrjournal.com. <https://csrjournal.com/index.php/csrjournal/article/view/50>
- The Broadband Commission for Digital Development. (2024). *Cyber violence against women and girls a report by the UN broadband commission for digital development working group on broadband and gender*. https://networkedintelligence.com/wp-content/uploads/2019/02/Cyber_violence_Gender-report.pdf
- Udai, N., & Sharma, D. (2025, April 15). *Navigating the digital landscape: A study on cyber safety and digital harassment in college campus among female students*. Ssrn.com. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5231387
- Vakhitova, Z. I. (2025). Cyber-Routine activity theory. *Oxford Research Encyclopedia of Criminology and Criminal*



- Justice*, 1(1).
<https://doi.org/10.1093/acrefore/9780190264079.013.784>
- Wikström, P.-O. H. (2009). Routine activity theories. *Oxford Bibliographies*, 1(0).
<https://doi.org/10.1093/obo/9780195396607-0010>
- Wilk, A. van der. (2021). *Protecting women and girls from violence in the digital age*. <https://rm.coe.int/the-relevance-of-the-ic-and-the-budapest-convention-on-cybercrime-in-a/1680a5eba3>
- Yar, M. (2005). The novelty of “cybercrime”: An assessment in light of routine activity theory. *European Journal of Criminology*, 2(4), 407–427. <https://doi.org/10.1177/147737080556056>
- Zahoor, R., & Razi, N. (2020). Cyber-Crimes and cyber laws of Pakistan: An overview. *Progressive Research Journal of Arts & Humanities (PRJAH)*, 2(2), 133–143. <https://doi.org/10.51872/prjah.vol2.iss2.43>

