CYBER CRIME IN PAKISTAN; DETECTION AND PUNISHMENT MECHANISM

Ubair Anjum

Pakistan Institute of Development Economics, Quaid-i-Azam University Campus، Islamabad, Islamabad Capital Territory 44000, Pakistan, mubairanjum@gmail.com

ORIGINAL SCIENTIFIC PAPER

ISSN 2637-2150
e-ISSN 2637-2614
UDK 343.533::004.056(540)
DIO 10.7251/STED0220029A

Paper received: 25.10.2020.
Paper accepted: 20.11.2020.
Published: 30.11.2020.
http://stedj-univerzitetpim.com

Corresponding Author:
Ubair Anjum, Pakistan Institute of Development Economics, Quaid-i-Azam University Campus Islamabad, Islamabad Capital Territory 44000, Pakistan, mubairanjum@gmail.com

ABSTRACT

"Cyber Crime in Pakistan; Detection and Punishment Mechanism" addresses improvement of public health and safety policies by focusing on enhancing knowledge about cybercrime, women victimization, the pattern of time spent on the internet, sexual harassment and cyber-bullying and the effect of socio-demographic factors on cybercrime. A quantitative, self-selected research study designed by the researcher and utilizing a voluntary, anonymous internet survey consisting of open and closed-ended questions targeted students attending large universities in Pakistan (N=400), based on Routine Activity Theory (RAT). The results were analyzed through SPSS via directing descriptive statistics, Cronbach's alpha, and regression analysis to confirm the validity and internal consistency of data and verification of the hypotheses. Results depicted women represent the largest group impacted by cyber abuse. Single women, young adults, and employed students demonstrate increased rates of victimization. Frequent usage of social media may account for increased victimization for women. Time spent online and deficient knowledge of cyber protection measures are positively correlated with digital victimization. Respondents report on inadequate effective and affordable cyber protection and ineffective responses by agencies to cybercrime. Based on the results garnered, and supported by Public Policy Theory, Cybersecurity policies have been proposed to Pakistan's government.

Key Words: Cybercrime; Cyber victimization; Cyber Violence; Cyber Laws; Routine Activity Theory; Public Policy Theory.

INTRODUCTION:

The overall domain of technology has been changed entirely after the www (World Wide Web) and online computer connectivity, which is considered mandatory for all aspects of business and corporate world. Before the internet revolution, both private and public organizations kept their highly confidential information in the form of physical documents (Waldo, Lin, & Millett, 2010). The physically stored information makes sure that the information is not easily available to anybody to take benefit from it, but their security was not much ensured. However, the new paradigms have

generated huge data banks with all kinds of information rather than physical record keeping. Although the data banks are safer way to keep information as compare to physical record keeping, but all of the information which is available online even under strict security measures has the high risk of being attacked. The reason of this risk is day by day advancement in technology and increased ratio of web users (Anderson, & Rainie, 2018). Cybercrimes have diverse ranges and categories; thus, the victims of the cybercrimes reveal to be free of the age limits and the social backgrounds. Moreover, these crimes do not require expertise to commit; rather with the technological advancements the world has become global village and thus, the different ways to access the people easily across the globe and hacking their information have also been generated. In recent era everyone has an easy access to the internet but unfortunately this easiness has been used destructively as well, as more use of technology is leading to more cyber victimization. The people have 10 times higher threat of being victim of cyber-crimes as compared to the physical crimes (Nurse, 2018).

Cyber space or commonly known as internet is the most used medium these days, in all aspects of human lives. It is involved in all domains whether it is business, entertainment, banking, education, logistics, military services or research. Virtually no human activity is possible without the usage of internet technologies (Crowther, 2017).

The development of society based on the internet technologies has introduced great advantage in all aspects of human lives. Flow of information across the globe and knowledge accessibility for common man has completely changed the face of modern society. Online shopping, online banking, voice over internet protocols for telephony services is a few examples of modern internet advancements. All these technical developments in the daily lives of common man have provided unhindered access to the information especially to the people from third world countries. With this level of information, the growth and advancement in society is facing a new and serious threat related to this zone. The information is now freely available on the internet. Most of the infrastructure like traffic control, water supply, air conditioning is completely dependent on the internet connectivity and computer networks. So, attack against these services and informational infrastructure may leads to disastrous and critical ways of harming (Gluschke, Hakki, Macori, & Leszczyna, 2018). Other than this, states that as a result of technological advancement the transition from paper money to the credit card devolution and seamless expansion of instantaneous and immediate global markets have completely transformed the domains of crimes, and changes it beyond the perspective of place people and identity (Smith, Cheung, & Lau, 2015). According to the survey, Kemp, S. indicated that in 2011 one third of world's population near 2.3 billion people have accesses to the internet which have become 4 billion in 2018 (Kemp, 2018). Moreover, among 60% of these internet users belong to the developing countries and 45% of them have ages under 25. According to him, in 2017 the mobile broadband subscriptions reached up to 70% of the total's world population. He further estimated that, after the year 2020 the ratio of network devices with humans will be six to one.

With passage of time it has been detected that more cybercrimes left more victims as well. According to Waghole, S.N., every single person using internet is now having 20% more chances of being robbed through its computer as compare to the street robbing, out of ten one adult is a victim of cybercrime and hacking attacks and online frauds are just few examples related to the cybercrimes (Waghole, 2019). According to him, all these crimes are committed on large scales and group of people with different technological backgrounds are involved in it who are normally experts of internet. Online fraud is the most prevalent form of crime as these days as compare to the normal theft. As compared to conventional crimes, victims

of cybercrimes are drawn from all ages, all backgrounds and all parts of world (Broadhurst, Grabosky, Alazab, Bouhours, & Chon, 2014). As far as the gender is concerned it is also evident that women are more likely to be the victims of cybercrime as compare to the men. A news article by Jurgita Peciuriene, EIGE's program coordinator for gender-based violence reported that effect of this violence has far more traumatic impacts on the lives of women (Peciuriene, 2017).

Despite of the fact that cybercrime is the term used frequently these days; it is hard to explain the term precisely because of its occurrence in multiple consequences. Like conventional crimes, cybercrimes can occur in numerous scenarios and have different facets. For example the council of Europe's Cybercrime treaty uses the term that refers to the criminal activity perform against the data content and copyright violation. Zeviar-Geese, stated that cyber-crime is a broader term and includes all the activities like child pornography, fraud, unauthorized access to the data and cyber-stalking Gordon & Ford, presents that cybercrime has two types; type 1 and type 2 (Zeviar-Geese, 2005; Gordon & Ford, 2006). Type 1 crimes are more technical in nature like bots Trojans or phishing scams. On the other hand, Type 2 crimes include; sexual harassment, black mailing, planning terrorist activities online. These types of crimes are facilitated using different chat software (*Table 1*).

Table 1. Types of Cyber Crime (*Gordon and Ford, 2006)*

Type No	Example	Software Used
1	Phishing scams	Email
1	Identity Theft	Trojan, key loggers
1	DDOS	Bots
2	Cyber terrorism	Chat software, Encryption
2	Cyber stalking	Messengers, Emails

Crime prevention strategies comprised of the measures minimizing the occurrence of crime and also mitigate the potential destructive impacts on people and society. Almost 40% of the countries have the policies and national laws designed for the prevention of cybercrimes. Rests of 20% countries across the globe are on their way to design the effective policies for prevention of cybercrimes. There are multiple dimensions of these policies based on different factors included educational level of people in country, law enforcement capacity of government, leadership qualities and strong knowledge base of cooperation among private and government sectors. In many countries the cybercrime strategies are integrated with cyber security. It is clearly seen in last decade that the ratio of cybercrimes is more and more immense and this is one issue that should not be ignored in terms of its prevention. Table 2 presents the top 20 countries having high ratio of online frauds.

Cyber-crime has been studied out generally in most of the studies without categorizing the victimizations in terms of the gender or age groups (Arfi, & Agarwal, 2014). This inclusive research study has been carried out in order to clarify the category of genders in cyber-crime victimization specifically in the perspective of Pakistan. Though, there are so many studies in perspective of the developed states; Europe, United Kingdom and the United States of America concerning the cyber-crime but the changing trends and the living mechanism of states diversify the effects of cyber-crime victimization for each of the geography inclusively. The ratio that how many women victims have been target of cybercrime is not exact. Moreover, there are discrepancies in measures and initiatives by the Pakistan to deal with the issue of cyber-crime and to overcome of it, so it is a central problematic hallmark for the world as well.

Rationale

The need of the cyber capability's infrastructure development is mandatory in domains of Pakistan because of ineffective

operationalization of the existing measures, as Pakistan had faced the loss of the "US $ 6 million" in 2018 due to cyber-attacks (Khalil, 2020). This study is about to present a comprehensive analysis of the unfortunate victimizations in cybercrime and the distinctive preventive estimates that have effectively taken for ceasing the cybercrimes as well, by focusing the geographical region, "Pakistan", as the under-study state is revealed to have increased issues of cyber-crime and insufficient approaches to overcome of this problem.

Table 2. Cyber Attack Rates for the Top 20 Countries (Adopted from Morgan, 2017).

Sr.	Countries	Total Attacks	Sr.	Countries	Total Attacks
01	Canada	**3164**	11	France	**368**
02	India	**2819**	12	China	**366**
03	United Kingdom	**1383**	13	South Africa	**349**
04	Australia	**989**	14	Italy	**291**
05	Mexico	**632**	15	Pakistan	**276**
06	Russian Federation	**594**	16	Netherlands	**266**
07	Brazil	**558**	17	Malaysia	**265**
08	Germany	**466**	18	United Arab Emirates	**259**
09	Philippines	**453**	19	Spain	**248**
10	Japan	**413**	20	Argentina	**238**

Theoretical Background

This current study is based upon Public Policy Theory, which is generally understood as a contextually-based course of action undertaken by a government in response to a particular public problem or issue. In this study, the policy refers to governmental cybercrime deterrents. I utilized Routine Activity Theory (RAT) as the basis of my research. According to RAT, three components must be present for a crime to occur: Availability of an appropriate target, a motivated criminal offender, and non-availability of a proficient "guardian" to prevent the crime occurrence. This theory includes the routine activities of both the victim and the perpetrator, attending to areas where the activities overlap, which provides the opportunity for crime to occur. Understanding where the intersections occur allows for a preventative course of action to reduce the likelihood of crime occurring (Figure 1 Analytical Framework).

Hypotheses

H_1: Respondents with increased knowledge about risks and safeguards of internet use experienced lower rates of cybercrime victimization as compared to those without reported internet safety education.

H_2: The rate of cybercrime victimization of women is higher than that of men, across age groupings.

H_3: Time spent online is positively correlated with cybercrime victimization.

H_4: The rate of sexual harassment and cyber bullying is positively correlated with frequent use of social media and associated internet communication.

H_5: Specific socio-demographic factors, such as age and gender, have significant relationships with both the types and the frequency of cybercrime victimization.

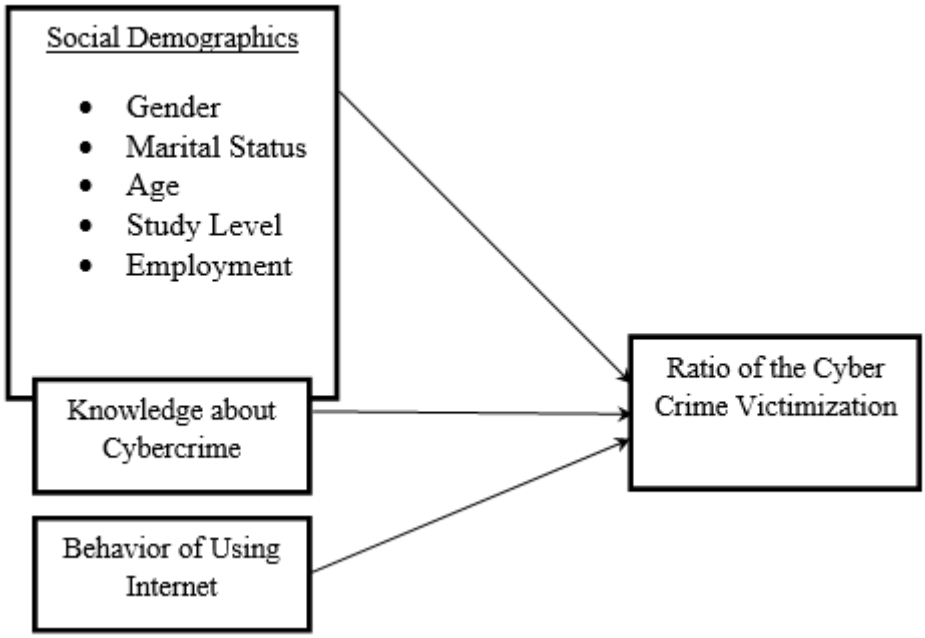

Figure 1: Analytical Framework

LITERATURE REVIEW

The term 'Cybercrime' first entered public usage after author Will Gibson used it in his 1985 popular science fiction novel, "Neuromancer" (Lavigne, 2008). This term has entered the common lexicon due to its recurrent usage in a wide range of contexts (Jamil, 2006). Thus, Navneet K., argued that while any illegal and punishable acts by governments or industries establishments are known as crime, of all of the multitudinous forms that crime can take, the most prevalent are cybercrimes, those conducted on the internet (Navneet, 2018). Virtual crimes are spreading at an exponential rate, due to fast emerging technology and applications that are not yet accounted for in the existing safeguards protecting internet users. Existing frameworks and technology used by law enforcement are often inadequate for novel forms of cybercrime, complicating investigations.

Classification of Cybercrimes

A variety of classification methods have been formulated to quantify specific types of cybercrime. Gordon & Ford presented two particular terminologies for categorizing cybercrime; "cyber-dependent crime" and "cyber-enabled crime" (Gordon, & Ford, 2002). Cyber-dependent crime is conducted with and through the engagement of the computers or other forms of ICT; including crimes encompassing hacking, DDOS (Denial of Service) attacks or insertion of malicious and mischievous software. Cyber-enabled crimes are pre-existing types of crime that are enhanced in scope and intensity thorough the internet. Economic and social networking fraud falls under this category (McGuire, & Dowling,

2013). Navneet, K., further classifies cybercrimes into three broader typologies of cybercrimes: Cybercrimes against individuals (e-mail harassment, phishing, spamming, cyber-defamation, cyber stalking, salami attacks, computer sabotage, and malware), cybercrimes against property (intellectual property crime**,** cybersquatting**,** cyber-vandalism**,** hacking into systems**,** altering way of unauthorized**,** logic bomb**,** trojan horse) and cybercrimes against organizations (hacking, password, denial attack, virus attack, mail bomb) (Navneet, 2018). Smith, classify cybercrimes as semantic, syntactic and blended (Smith, 2010). Semantic crimes refer to social networking, syntactic crimes are purely technical and often involve self-replicating viruses that the victim unwittingly opens, as often seen in ransomware attacks, and blended crimes combine elements of both. The strategy often employed in blended crimes involves the perpetrator contacting the victim and offering the solution to a plausible problem persuasively enough that the victim willingly provides access to personal and financial information to the criminal. In this case, the personal information stolen from victims is sold and used to commit further frauds.

Economic Impact

Cyber offenders are perpetually creating novel methods of obtaining data from citizens, businesses and governments through illegitimate means, in order to formulate new methods of attack and evasion. Morgan presented a list of the top 20 countries (Table 2) with the highest cybercrime victimization rates (Morgan, 2017). According to Huff et al. cybercrime has become a requisite cost of some virtual economies (Huff, Desilets, & Kane, 2010). The most established and competent hackers in these illegal economies are also enriching the cybercrime ecosystem, which includes illegal activity through a hidden "darknet" form of the internet, using widespread cyber-attack methods such as malware, and funded through virtual crypto-currency, such as Bitcoin, which can function as digital money laundering platforms. Some of these hackers have micro-enterprises while others exist much like legitimate business conglomerates. The scale of these operations allows them to recruit highly skilled IT workers (Bryan-Low 2012). The two economies with highest cybercrime victimization rates are South Africa and China. As the sophistication and rapidity of cybercrime attacks increases, numerous countries have designed and implemented methods of cyber warfare against them (Lewis, 2018). It has been mentioned by Porche 2019, that a survey conducted with the world's top internet experts concluded that China has the highest capability for combating cyber warfare. Russia and the USA are tied for second place, while Israel comes in third for the most efficient technologies for neutralizing cybercrimes. Despite their apparent success in fighting cybercrime, Poulsen 2018, stated that 66% of adult consumers are more concerned about the risk of cybercrimes than the risk of any physical crimes in the US.

Social Media and Cybercrime

Cybercrime victimization has received intensive study in the past decade, particularly with regards to online harassment (Jones, Mitchell, & Finkelhor, 2013). According to the Federal Bureau of Investigation (FBI) almost 288,012 cases of cybercrimes were reported in the USA in 2015; of these, 49% were reported by women (Federal Bureau of Investigation [FBI], 2016). Morgan and Kena 2017, also found that 60% of the harassment in online groups specifically targets women. New forms of social interaction, originated by Facebook, have given criminals, hiding behind a false persona, ready access to people innocently engaging in social interactions, oblivious of the other users' true identities and motives. Predators often groom their victims through false sympathy, and encourage the victim to become emotionally dependent on them in order to gain access to their personal and financial information. Facebook was launched in 2004, and now it claims 2.19 billion active users (Statista, 2018). In the

wake of Facebook's success, other social networking sites have proliferated, often catering to specific demographic groups. Dating and match-making sites have also proved fertile ground for fraud and scams. It is estimated that one in five relationships now start online. According to the study of Mendes, Ringrose, & Keller 2019, women of all countries face more intensive and persistent forms of harassment than men. Females are often harassed and humiliated over personal attributes, and they are stalked by sexual predators at a far greater rate than men (Duggan, 2014). Many studies have examined cyber bullying and other cybercrime victimization of young women in particular (Oksanen & Keipi 2013). Results of most of these previous studies demonstrated that the young women between the ages of 18 and 25 years are most prone to suffering abuse and victimization, usually in the form of sexual harassment and unwanted attention, at rates far greater than any male cohort (Helweg-Larsen, Schütt & Larsen, 2012).

Cybercrime in Pakistan

Cybercrime operations in Pakistan are markedly different from the prevalent forms in many countries. In contrast with lucrative cybercrimes such as hacking, infections, viruses and worms, the most widely documented cybercrime in Pakistan is online harassment and defamation, especially for women. Young women in Pakistan typically share pictures and videos online with their friends and romantic interests. Friendship with members of the opposite sex is culturally frowned upon, and purported male "friends" may harrass the women who view them as friends in order to push them into more intimate relationships. According to the report of Telecommunication 2017, there is an astonishing difference between the ratios of men and women owning the cell phones and ICT in Pakistan and ratios of their reported victimization. An estimated 84% of the men and 64% of women own personal cell phones in Pakistan, and 75% of internet users are male. Despite this disparity, female victims account for the bulk of online harassment, stalking, and other forms of virtual viciousness (Sheikh, 2013). The Federal Investigation Agency of Pakistan (FIA) indicated that out of 3025 recorded cases in 2015, 45% of personal, social app cyber-attacks were made against women.

Women and Cybercrime in Pakistan

Digital Rights Foundation (DRF) surveyed cyber victimization using a sample of 1400 females for their investigation, focusing primarily on those reporting frequent use of social media (Digital Rights Foundation [DRF], 2017). Study results indicated that 70% of women expressed fear that photos they had posted on social media within the past two years would be exploited for harassment. 40% of the women in the survey described personal discomfort and harassment through message apps. This study, in the context of Pakistan, revealed the high rates of female cyber victimization. Moreover, according to DRF 2017, in an analysis of calls made to the country's cyber harassment helpline, the most significant kinds of provocation identified by Pakistani females fell into multiple categories, including intimidation (20%), blackmail (21%), unwanted messages (12%), and absence of information comprehension (19%).

Culture and Cybercrime

The two primary personal risk factors for female victimization by cyber criminals are ignorance about cyber safety, especially when compared to women working employed in the fields of science and engineering, and cultural and familial restrictions imposed on women. The predominant culture in Pakistan revolves around family. Both the family, in particular the father and society treat women as children in need of guidance and protection. They are sheltered to the extent of carefully monitoring women activities, and by doing so, they the opportunities for real life socializing that would normally cause a woman to develop a healthy level of skepticism and caution regarding how and with whom they communicate on the

internet. Unfortunately, the virtual open society and freedom of the internet may prove to be a powerful attraction for these young women, leading them to divulge more highly personal responses and activities than are allowed in Pakistani society. Their lack of knowledge about internet safety is frequently compounded by fathers restricting approved employment, and higher education opportunities in technical fields, which would enable them to make wiser decisions on the internet. According to FIA's National Response Center for Cyber Crimes, during 2015, 3,000 cases of online harassment against women were reported. 45% of these cases were in the form of online harassment through social media (Al-Jazeera, 2016).

Government Responses to Cybercrime in Pakistan

Cybercrime legislation in Pakistan is currently managed through the "Prevention of Electronic Crime Act", 2016. Although this framework is more comprehensive than previous legislation, it does not cover all of the domains of cybercrime currently deployed in Pakistan, and often it appears to exist more on paper than in practice (Usman 2016). According to DAWN newspaper's October 23, 2018 report by Qarar 2018, regarding the statistics of FIA, cybercrime was at a record high in 2018, with harassment and blackmailing cases involving women sharply increasing over the past three years. According to FIA's cyber-crime call center records, 2,295 requests for assistance were made, resulting in 255 active cases and 209 captures in 2018 (Qarar, 2018). Their statistics for 2017 showed 1,290 calls, 207 cases enrolled, and 160 captures made. Moreover, according to these reporting figures for 2016 revealed only 514 calls, 47 cases and 49 arrests. Additionally, Malik 2018, has presented multiple reasons for cybercrimes in Pakistan, including lack of risk awareness, insufficient preventive measures, absence of effective policies, lack of an educated workforce in police and enforcement agencies, slow government responses through legislation, and lower standards for protective programs such as ant-virus and malware for ICT. Additional system-wide issues include the lack of a realistic economic budget devoted to cybercrime, insufficient cyber-designated resources, and poorly coordinated research and development.

METHODOLOGY

Research methodology is the overall plan stipulating the rationality of the theory development process, and an applied framework to conduct the research (Remenyi, Williams, Money, & Swartz, 1998). Therefore, according to Mohajan 2017, research methodology provides the criterions to organizing, arranging, structuring, and leading the research, and the methodological choices based on the research paradigm utilized by the researcher. The focus of this study is the investigation of victimization in the domain of cybercrime within the context of Pakistan, through use of quantitative measures, and following the 'positivism' paradigm. Positivists follow an operational approach to research, which includes having a clear topic of research, hypotheses, and the appropriate methodology to test those hypotheses (Churchill, Brown, & Suter, 1996). This study follows the quantitative deductive approach. Utilizing this approach will permit the testing of hypotheses based on cause and effect relationships among the variables of the study, due to its highly structured nature (Saunders, Lewis, & Thornhill, 2009).

Population and Sampling

The segment of the population considered for this current research includes students from the large universities rated in the top 30, as ranked for academic excellence in Pakistan. Higher Education Commission of Pakistan. A total of 400 self-selected students were surveyed for this purpose. These students were considered the target population due to the amount of time they spend online participating in social websites, which gave them the greatest probability of having experienced

cybercrime victimization. It was considered most expedient to focus the survey on this predominantly young, educated, and relatively affluent population, due to their increased likelihood of representing the variables associated with the study. My rationale for these assumptions lies in the fact that these students are already users of ICT for university courses, and are more likely to actively pursue information about the global online society. Teens and young adults are more active on social sites, and confidence stemming from studying at a top university may result in overestimating their own understanding of associated risks. Additionally, some of these students may be living away from home for the first time, without parental oversight, or adequate prior knowledge regarding cyber safety and coping with cybercrime if it occurs. These identifiable risk factors indicate that university students as a group run a higher risk for cyber victimization as compared to the general population.

This research study utilized a non-probability sampling technique. The reason for selecting non- probability sampling was due to the fact that the population is quite large, and the precise size of population was unknown (Alvi, 2016). The volunteer, or self-selection, sampling technique was further utilized here because of its appropriateness for the focus of the study. Respondents were targeted for this sampling technique based on their own willingness and interest in becoming part of the study, as a way to obtain precise information regarding the demographics of cybercrime in Pakistan (Abrams, 2010). Recruitment was conducted online through a variety of apps, which included social websites, e-mails, direct messaging, etc., where students were likely to be actively engaged. Therefore, due to the self-selection of respondents, it was not possible to utilize the equal probability of selection technique, commonly used for probability sampling.

Sample Size

For the purpose of this study, 30 universities were targeted, and 400 students responded to the survey. The sample size of 400 students also satisfied the requirement of sample size for an online survey (Krejcie, & Morgan, 1970). According to their formula, 285 responses are sufficient for a quantitative study, and for an unknown population, when the hypotheses are tested on the basis of the proportion of the population, which is expressed as 0.5 (50%) with 95% internal confidence, and a margin of error of 5% (0.05).

Sample Selection Formula

$$"n = \frac{N}{1 + Ne^2}"$$

Where:

n - Sample Size
N - Population
e = a = 0.05 (5%)

Thus, 400 is an adequate and sufficient sample size for quantitative research study.

Data Collection and Analysis

This study is based upon the voluntary survey method, in order to collect the data from students attending top ranked universities with high enrollment rates in Pakistan. This survey approach accumulates important explorative and vital information from this target population. A questionnaire, developed by the researcher, was used for data collection regarding cybercrime and cyber victimization to authenticate the study results. Online surveying methodology was utilized to capture data from the targeted population, and anonymity helped to insure both an adequate population of respondents and honesty answering the survey items. Additionally, online data collection increased the timeliness of the results by overcoming issues related to respondent convenience and geographical constraints (Andrews, Nonnecke, & Preece, 2003). This questionnaire comprises both open and close ended questions. A prior sample test of 20 questionnaires was conducted through

a pilot study, to confirm the reliability and validity of the research instrument, and to remedy any deficiencies at an early stage. Accurate understanding of the questions by respondents was ensured by obtaining responses on the test questionnaires, then adding and calculating the responses in dummy tables. The internal consistency of the survey items was ensured at this stage, with a Cronbatch's coefficient greater than 0.7 for each item investigated. After pilot testing, a trial run was completed with the actual data.

Data analysis was accomplished through SPSS, and findings were interpreted using Descriptive Statistics, Frequency Distribution and Reliability Analysis. In the data analysis, graph charts and bivariate tables are used to visualize the results for each construct of the study with collected data. For the purpose of this study, descriptive analysis involves the representation and interpretation of the results in the form of bar graphs presenting the statistical outcome of the responses given below.

RESULTS

Multiple socio-economic factors were tested for correlation with cybercrime victimization, including gender, level of higher education, employment status, marital status, geographical location, including type of housing, reporting cybercrime to authorities, and security software usage.

Descriptive Analysis

Age and Cybercrime Victimization

The data collected regarding cybercrime awareness among the university students, and the results are presented in Figure 2. In terms of cybercrime awareness, just 23.75% of the respondents reported awareness of cyber-enabled crime, while 31.75% indicated awareness of cyber-dependent crime. Only 8.75% said that they are aware of both kinds of cyber-crimes, but 75% indicated ignorance of both cyber-enabled crimes and cyber-dependent crimes (Figure 2). These ratios demonstrate extremely low levels of awareness regarding the terminology for cybercrimes among university students.

Multiple socio-demographic factors were tested for correlation with cybercrime victimization, including gender, level of higher education, employment status, marital status, location (geographical location), reporting to law enforcement agencies and security software usage.

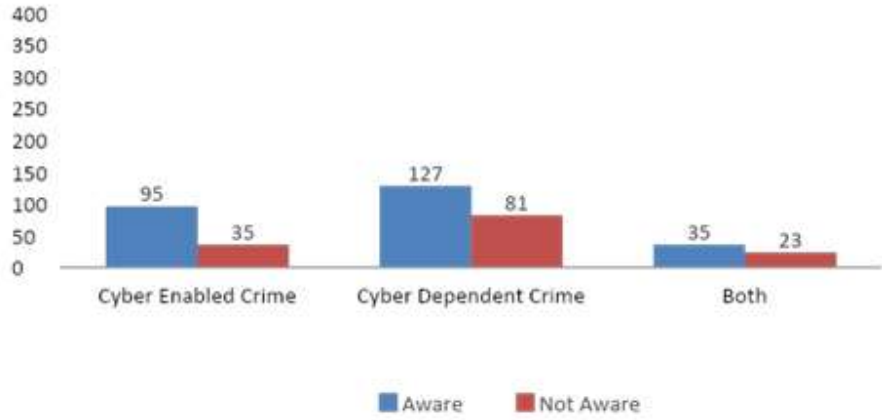

Figure 2: Awareness about Cybercrime

Gender and Cyber Crime Victimization

The results for correlation between gender and cybercrime victimization have been presented in a bar chart (Figure 3).

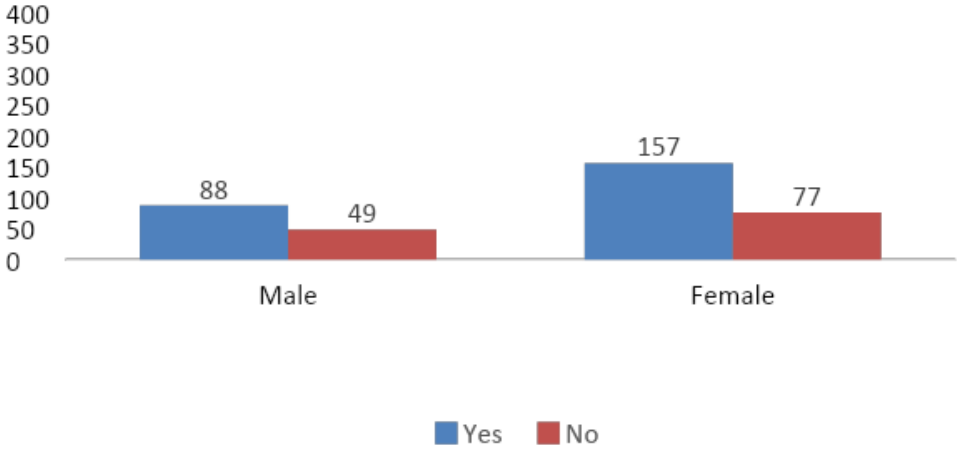

Figure 3: Gender and Cybercrime Victimization

This portion of the study revealed that among 400 respondents, 22% of males reported cybercrime victimization. In contrast, 39.25% of female respondents indicated that they have been victims of cybercrimes. On the basis of all collected data, 61.25% of respondents reported incidents of cybercrime victimization, with the number disproportionately represented by female respondents (Figure 3).

Age and Cybercrime Victimization

For the purpose of understanding the relationship between the variables of respondent's age and cybercrime victimization, four age subgroups have been established, based on the average age of students ranging from Bachelor's Degree class levels to Doctoral Degree programs. The age categories are as follows: Less than 20 years, 20 to 30 years, 31 to 40 years and above 40 years of age (Figure 4).

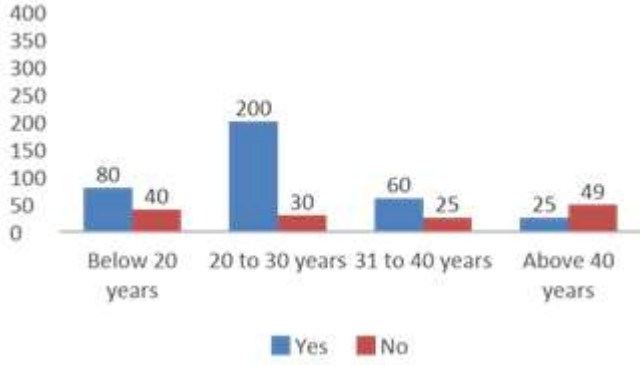

Figure 4: Age and Cybercrime Victimization

For students below 20 years old, 20% have been victims of cybercrime. 50% of victims were students between 20 to 30 years of age, 15% of victims were between 31 and 40 years old, and 6.25% of victims were above 40 years old (Figure 4.3). These results reveal that the most highly victimized age group for cybercrimes were respondents between 20 and 30 years of age.

Course level, Employment Status and Cybercrime Victimization

The university course level of the respondents was also separated into full time or part time students, and examined for the influence of these variables on cyber victimization (Figure 5). Results (see figure 5), show that 19.25% of the students who are engaged in full time study believe that they are exposed to cyber-attacks. On the other hand, of the part time students, 36.25% stated that they have already experienced cybercrime. The rate of cybercrime victimization by part time students is far greater than that of full-time students.

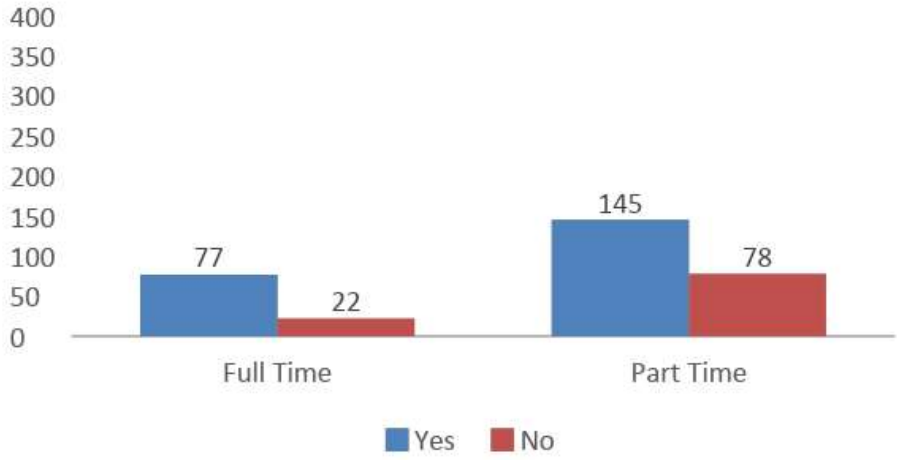

Figure 5: Study Level and Cybercrime Victimization

Employment and Cybercrime Victimization

The results (Figure 6), demonstrate that students who are not working (8.5%) or working part time (5.75%) has faced few cybercrimes as comparison to those working full time. For students who work full time, 29.5% said that they believe that they have been targets of cybercrimes. According to these respondents, the double demands of simultaneous work and study result in frequent engagement with multiple activities via web or internet.

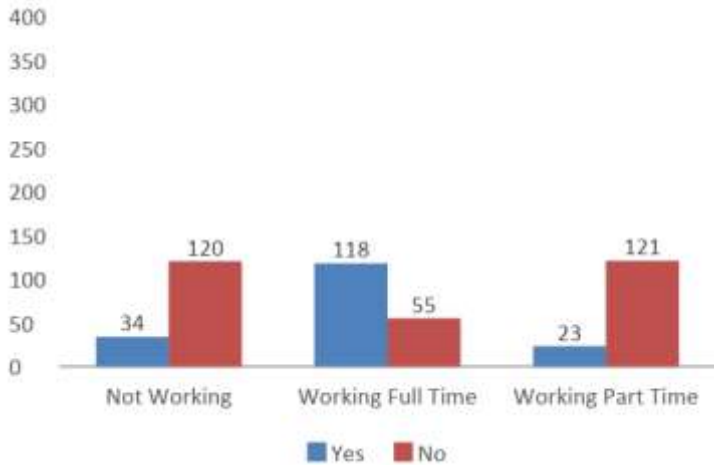

Figure 6: Employment and Cybercrime Victimization

Marital Status and Cybercrime Victimization

Marital status has been categorized as single, married, divorced or widowed, in order to determine the categories most frequently targeted for cybercrime. For this study, students of all levels, including Bachelor's, Master's and Doctoral degree programs, are the potential respondents of the study. Considering this point, the categories of divorced and widow were also generated, to take into account the greater age of Doctoral students. The results have been presented in the form of a bar chart (see Figure 7).

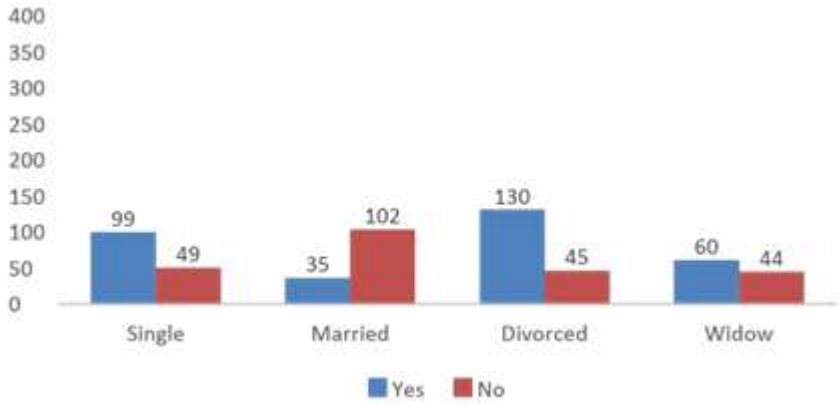

Figure 7: Marital Status and Cybercrime Victimization

The results show the following percentages: 24.75% of single people responded positively regarding whether they have encountered cybercrime in different forms, 8.75% married respondents have experienced cybercrime, and 32.5% of divorced respondents reported victimization through online harassment or bullying from their ex-spouse. An additional 15% of widows indicated that they had dealt with varying types of cybercrime.

Location and Cybercrime Victimization

The residence locations of the ***respondents*** were also tested in association with cybercrime victimization. The domicile categories included on campus residences, off the campus and within the same city as their university, and off the campus in rural areas (Figure 8).

According to the results, 13.75% of victims resided on campus. In case of off-campus residences located in the city, 16.5% said that they have been victimized by cybercrime, and finally, in case of off-campus commuters in rural areas, 5.75% reported that they have been victims of cybercrime. The rate of those not experiencing cybercrime is significantly higher than the rate of victimization in all three of the above variables under investigation. Thus, the negative correlation between location of residence and cybercrime victimization has also been evaluated.

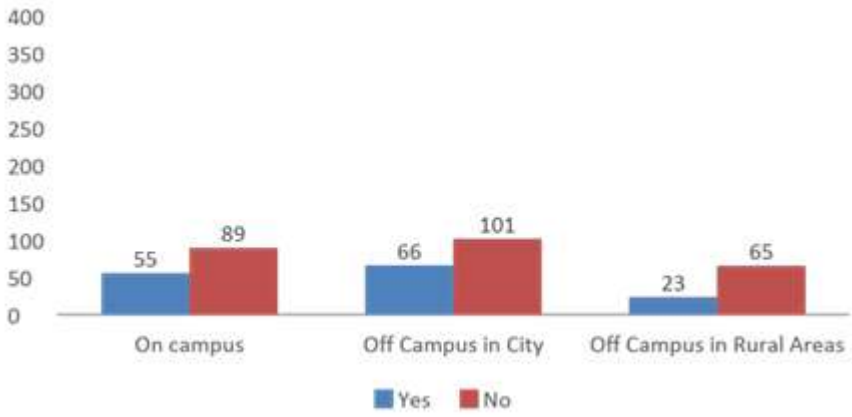

Figure 8: Location and Cybercrime Victimization

Reporting to Law Enforcement Agencies

Cybercrime victimization demands timely reporting to law enforcement agencies in order to respond effectively to the problem case by case, and within society as a whole, in order to monitor trends and patterns, and evaluate the efficacy of established responses.

According to the results (Figure 9), almost 77% of respondents stated that they have never reported their experience of cybercrime to a law enforcement agency. The remaining 23% attempted to report cybercrime to law enforcement agencies, but were dissatisfied with the efficiency and responses of those agencies.

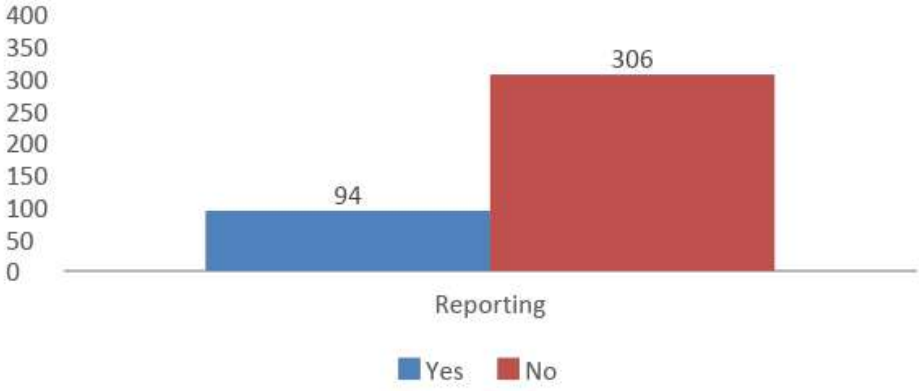

Figure 9: Reporting to Law Enforcement Agencies if Victimized

Usage of Security Software

The presence of ***effective cyber security*** software installed on a person's ICT is one of the strongest deterrents to cybercrime victimization. For the students surveyed in this study, the following results were obtained regarding whether or not some form security software was ***utilized*** to prevent cybercrime issues (Figure 10). Almost 66% of the total respondents do not use any type of security software. The remaining 33% used some kind of software, including anti-virus programs. This lack of installed cyber security programs presents a substantial risk for future cyber victimization.

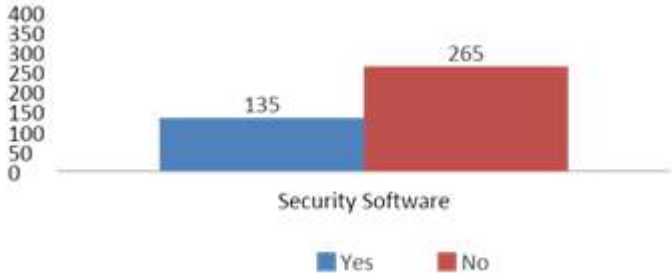

Figure 10: Usage of Security Software in Preventing Cybercrime Victimization

Types of Cybercrimes Faced by Respondents

The frequencies and percentages of different types of cybercrime have been presented in Table 3. Cybercrimes reported most often by victims involved receiving threats centered on their personal photos posted on social media (32%). Almost 26% of the respondents received anonymous phone calls and text messaging (SMS), and 59% of the respondents faced the issue of fake profile**s and misuse of their profiles.** All of these crimes represent some form of social media-related incident, pointing to the substantial risks involved with unwary use of these sites.

Table 3. Rates of Types of Cybercrimes

Types	Frequency	Percentage
Phishing emails	7	3.52
Hacking of accounts	12	7.34
Threatening calls for photos uploading	43	22.01
Credit card-based frauds	12	6.92
Stalking	21	15.71
Online harassment	35	18.01
Spam emails	26	14.01
Anonymous calls and SMS	53	26.34
Fake profile creation	59	28.72
Photo Circulation	33	16.09
Threatening about the Photo circulation	67	32.01

Statistical Descriptions Using Statistical Calculations

Activities performed by respondents using Various ICT

The data under consideration examined the types of activities performed on the internet by the respondents using different forms of ICT, in order to understand the habits of students regarding internet access. Results have been presented in Table 4.

Almost 87% of respondents prefer to use their phones to access social networking sites, while 34% use tablets, 23% use laptops, and 18% use desktops. This is significant, because phones are the most portable and accessible form of ICT, making quick interactions relatively easy, without requiring forethought.

Table 4. Activities Performed Internet Users by type of by type of ICT

	Phone %	Tablet %	Laptop %	Desktop%
Social networking sites	87.01	34.2	23.21	18.09
Shopping	3.01	11.90	10.98	4.89
Sharing files	2.09	45.09	64.09	63.12
Game Playing	78.01	67.09	53.23	43.01
Online Banking	46.01	32.01	67.19	64.22
Music Downloads	45.45	57.98	78.91	76.09
Chatting	76.98	45.90	43.01	34.01
Emailing	3.09	34.94	65.90	14.90

Purpose of Internet Usage By respondents

Data has been collected to determine the purposes for using the internet by the respondents, in order to evaluate their reasons and patterns of use, and to thereby gain knowledge about commonly accessed internet sites where they could be exposed to cybercrime. The results have been presented in Table 5. According to the calculations, 24.63% respondents use the internet for social networking, 10.87% use for study, 3.23% use for online banking, 35.2 % use for official work, and highest percentage, 79.8%, of respondents use the internet to keep in touch with family and friends. According to these rates, it appears that social apps are where most of the cyber victimization cases are likely to arise.

Table 5. Reason of Internet Usage by Respondents

Reasons	Frequency	Percentage
Social networking	65	24.63
Study	18	10.87
Online Billings	10	3.23
Official work	140	35.2
Staying in touch with family and friends	139	79.8

Use of Social networking sites by respondents

For sake of the results evaluation, data has been collected regarding the pattern of use within social sites by the respondents, and the results have been presented in Table 6. Statistical values show that 70% of the respondents have one social media account, 22% of them have two accounts and only 3% of the respondents have three accounts. 89% of the respondents have been using Social Networking Services (SNS) for less than 5 years, while 6% of the respondents have been using these websites for less than 10 years. Only 1.3% of the respondents have accounts that are older than 10 years. 45% respondents have less than 100 online friends, 5% have a number of online friends ranging from 100 to 200, and only 0.91% respondents have more than 200 online friends.

Table 6. Use of Social networking sites by respondents

Social Network Sites (SNS)	Number	Frequency	Percentage
	One	101	70.92
Number of accounts	Two	29	22.01
	Three	9	3.09
	Below 5	91	89.1
Number of Years	5-10	12	6.20
	Above 10	4	1.3
	Below 100	43	45
Online Friends	100-200	9	5
	Above 200	2	0.91

Hypothesis Testing

Hypothesis 1: Knowledge about specific terminologies for types of cybercrime is sub-divided into two hypotheses.

Hypothesis$_{1A}$: Knowledge about specific terminology is important (table 7). The null hypothesis is not rejected according to value p=0.072 (Table 7). This demonstrates that it does not make any difference whether or not the respondent has knowledge about specific terminologies.

Table 7. Hypothesis$_{1A}$

Knowledge About Cybercrime terminology	Mean (M)	Standard Deviation (S.D)	t-value	p-value
cyber enabled	14.12	4.043	17.88	0.072
cyber dependent crimes	18.87	9.324		

Hypothesis$_{1B}$: Students without knowledge about cybercrime methods have reduced rates of cybercrime victimization (table 8). Table 8 shows the p-value is less than 0.05 which clearly rejects our null hypothesis and demonstrates that there is a significant relationship between a lack of knowledge about cyber risks and becoming a cybercrime victim. Respondents lacking any knowledge about cybercrime have an increased risk of becoming a cybercrime victim.

Table 8. Hypothesis$_{1B}$

Knowledge About Cybercrime	Mean (M)	Standard Deviation (S.D)	t-value	p-value
Well Aware	2.34	2.765	17.88	0.001
Not Aware	6.65	7.83		

Hypothesis 2: Women and men have an equal chance of becoming the victim of cybercrime (table 9). According to data in Table 9, the resultant p-value is 0.000, which is less than 0.05, and clearly rejects our null hypothesis. Data show that there is a significant relationship between gender and a cybercrime victim. Therefore, the mean value for the female respondents is significant as well (M=48.05, SD=25.97).

Table 9. Hypothesis 2

Gender	Mean (M)	Standard Deviation (SD)	t-value	p-value
Male	33.14	17.29	13.989	0.000
Female	48.05	25.97		

Hypothesis 3: Students who spend more time on the internet have lower risk for becoming a victim (table 10). According to data represented in Table 10, the resultant p-value is 0.0034, which is less than 0.05, and clearly rejects my null hypothesis, showing instead that there is a significant relationship between time spent on the internet, and likelihood of becoming a cybercrime victim. The mean value for respondents who spent more than 8 hours online is the most significant (M=53.01, SD=31.90).

Table 10. Hypothesis 3

No of Hours On internet	Mean (M)	Standard Deviation (SD)	t-value	p-value
2-4	17.21	8.29		
5-8	22.09	11.97	21.0998	0.0034
More than 8	53.01	31.90		

Hypothesis 4: Chances of sexual harassment and other forms of bullying is not increased by using social media and other online resources (table 11). According to Table 11, the resultant p-value is 0.000, which, being less than 0.05, clearly rejects our null hypothesis. Data shows that there is a significant relationship between harassment and social networking site, with a mean value T (M=61.65, SD=29.09).

Table 11. Hypothesis 4

Chances of Sexual Harassment and Cyber bullying because of using social media and online resources	**Mean (M)**	**Standard Deviation (SD)**	**t-value**	**p-value**
High	61.65	29.09	42.0654	0.000
Low	29.01	8.05		

Hypothesis 5: Null hypothesis

This hypothesis is further subdivided into seven hypotheses, in order to present the results for each of the socio-economic relationships separately. There is no significant relationship between socio-demographic features and cybercrime victimization. The demographics considered here are marital status, income level, study level and location of residence.

Hypothesis $_{5A}$: There is no significant relationship between marital status and cybercrime victimization (table 12). According to Table 12, the p-value is 0.061, which is greater than 0.05. Hence, the null hypothesis is not rejected, and instead data shows that there is no significant relationship between marital status and becoming a cybercrime victim.

Table 12. Hypothesis $_{5A}$

Marital Status	**Mean**	**Standard Deviation (SD)**	**p-value**
Single	56.07	21.39	0.061
Married	48.91	19.81	
N=400			

Hypothesis$_{5B}$: There is no significant relationship between income level and cybercrime victimization (table 13). According to Table 13, the p-value is 0.0721, which is greater than 0.05. Hence, my null hypothesis is not rejected, and shows that there is no significant relationship between income level and cybercrime victimization. Respondents from many types of work and income levels experienced cybercrime.

Table 13. Hypothesis $_{5B:}$ Income level

Income Level	Mean	Standard Deviation (SD)	p-value
Government Job	67.89	11.32	0.0721
Business	54.29	9.09	
N=400			

Hypothesis$_{5C}$: There is no significant relationship between study level and cybercrime victimization (table 14). According to Table 14, the p-value is 0.0508, which is greater than 0.05. Therefore, the null hypothesis is not rejected, and data shows that there is no significant relationship between the class levels. Both fulltime and part time students are facing cybercrime victimization. This variable is not important in answering the research question.

Table 14: Hypothesis $_{5C}$ Study Level

Study Level	Mean	Standard Deviation (SD	p-value
Full Time	12.001	3.10	0.0508
Part Time	19.09	6.002	
N=400			

Hypotesis$_{5D}$: There is no significant relationship between employment status and cybercrime victimization (table 15). According to Table 15, the p-value is 0.0009, which is less than 0.05. The null hypothesis is rejected. Instead, data shows that there is a significant relationship between employment status and becoming a cybercrime victim.

Table 15. Hypothesis $_{5D}$ Employment Status

Employment Status	Mean	Standard Deviation (SD)	p-value
Not working	4.19	3.10	0.0009
Working Full time	21.09	11.002	
Working part time	16.003	7.92	

Hypothesis$_{5E}$: There is no significant relationship between residence location and cybercrime victimization (table 16). According to data in Table 16, the p-value is 0.0621, which is greater than 0.05. My null hypothesis cannot be rejected, and data shows that there is no significant relationship between the respondent's location of residence and cybercrime victimization.

Table 16. Hypothesis $_{5E}$ Residence Location

Residence Location	Mean	Standard Deviation (SD)	p-value
On campus	6.99	3.10	0.0621
Off campus city	11.34	6.002	
Off campus rural areas	14.09	6.98	
N=400			

Hipothesis$_{5F}$: There is no significant relationship between age and cybercrime victimization (table 16). According to Table 17, the p-value is 0.00012, which is less than 0.05. Therefore, my null hypothesis is rejected, and data instead shows that there is a significant relationship between the respondent's age and the risk of becoming a cybercrime victim. Results in table 17 shows that students between 20 and 30 years of age face more cybercrimes in daily life.

Table 17. Hypothesis $_{5F}$ Age

Age	Mean	Standard Deviation (SD)	p-value
Under 20 years	7.087	3.10	0.00012
20-30	23.091	11.002	
31-40	14.981	5.98	
Above 40			
N=400			

Hipotesis$_{5G}$: There is no significant relationship between gender and cybercrime victimization (table 18). According to Table 18, the p-value is 0.0007, which is less than 0.05. The null hypothesis is rejected, and instead data shows that there is a significant relationship between gender and becoming a cybercrime victim. Results in the table show that the students who are female have a greater risk of becoming cybercrime victims as compared to men.

Table 18. Hypothesis $_{5G}$: Gender

Gender	Mean	Standard Deviation (SD	p-value
Male	9.233	5.012	0.0007
Female	32.09	17.90	
N=400			

DISCUSION

Hypothesis 1

The results of the first hypothesis indicated that respondents who are more knowledgeable have less chance of being cybercrime victims. This finding is supported by previous research studies (Van de Weijer & Leukfeldt, 2017).

According to my study results, respondents who have lower awareness about the types of cybercrimes and how these crimes are committed have a greater chance of becoming a cybercrime victim. According to the data analysis presented in Tables 7 and 8, there is a significant relationship between a lack of cyber awareness and becoming a cybercrime victim. Results show that the respondents who deny any knowledge about cybercrimes have a greater chance of becoming a cybercrime victim.

Hypothesis 2

My second hypothesis is designed to discover which gender is more affected by cybercrime. The proposed hypothesis was based on a previous research study exploring "whether the ratio of women is equal to men in case of cybercrime victimization" (Donner, 2016). According to Table 9, the resultant p-value is 0.000, which is less than 0.05, clearly rejecting the null hypothesis. Instead, my study showed that there is a significant relationship between gender and chances of being a cybercrime victim. The results show that female respondents have a higher risk, as compared to men, of becoming a victim of cybercrime. Moreover, the accuracy of these results is supported by descriptive analysis, (Figure 2), explaining that females are more often victimized by cybercrime, as compared to males.

Hypothesis 3

The third hypothesis was based on "The relationship between time spent online and chances of being a cybercrime victim". The proposed null hypothesis was that students who are spending more time on the internet have less risk of becoming a victim of cybercrime (Chao, & Yu, 2017). According to the analysis in Table 10, the resultant p-value is 0.0034, which is less than 0.05, and clearly rejects our null hypothesis; showing instead that there is a significant relationship between the amount of time spent on the internet and becoming a cybercrime victim. These results show that respondents who spent more time on the internet had greater chances of becoming a cybercrime victim.

Hypothesis 4

The proposed null hypothesis, "Chances of sexual harassment and cyber bullying are not increased by only using social media or other online resources" was also analyzed. According to Table 11, the resultant p-value is 0.000, which is less than 0.05, clearly rejects my null hypothesis, and shows instead that there is a significant relationship between harassment and the use of social networking sites. For respondents who report more activity on social networking sites, they have a higher chance of becoming a cybercrime victim. Results show that spending more time using social networking sites increases the likelihood of becoming a cybercrime victim.

Hypothesis 5

The primary hypothesis: "There is a relationship between socio-demographic features of respondents and cybercrime victimization". The proposed null hypothesis shows that there is no significant relationship between socio-demographic factors and cybercrime victimization. The demographics considered here are marital status (Table 12), income level (Table 13), study level (Table 14), employment status (Table 15), location of residence (Table 16), age (Table 17) and gender (Table 18). The results in this context show that certain socio-demographic features, including income level, residential location and study level, do not have any direct relationship with cybercrime victimization. On the other hand, marital status, employment status, age and gender all have significant correlations with cybercrime victimization.

Types of Cybercrimes Experienced by Respondents

Table 3 shows that the highest percentage of victims, almost 32%, faced threats about their photos circulating on social media. 3% of the respondents received phishing emails on a daily basis, and almost 7% of the respondents faced hacking of their accounts, and then having their accounts used by criminals for a variety of criminal activities. 22% of the respondents received threats about their personal photos, and most often the threats were coming from ex-husbands and other relatives seeing vengeance on the respondent. Generally, this kind of cybercrime activity is committed against women (99% of cases.) Almost 26% of the respondents reported receiving anonymous phone calls and SMS. 59% of the respondents dealt with the issue of fake profiles created with their name, which were then used to anger or embarrass them. Women responded higher regarding this issue, and of all the types of cybercrimes studied, these two types showed the greatest frequency.

Reporting Cybercrime to Law Enforcement Agencies

According to the results (see Figure 9), almost 77% of respondents stated that they have never reported cybercrime to a law enforcement agency. While the other 23% have tried to complain to agencies, they were not satisfied with the efficiency of these agencies. Non-reporting by the victims is the major factor driving the increase of cybercrimes, and thus, frauds, hacking and harassment is increasing on a daily basis (Van de Weijer, Leukfeldt, & Bernasco, 2018). Cybercrimes demand timely reporting in order to eradicate this problem.

Usage of Security Software

Figure 10 show that almost 66% of total respondents do not use any type of security software. The remaining 33% used some kind of software, including antivirus. Although the use of security software is highly recommended as a precautionary measure against hacking and fraud, many of the respondents claim that the free available software is of no value to protect them, and that most commercial software is based internationally, and not readily accessed or affordable for many web users in Pakistan.

Key Findings

The following key findings are significant in the context of this research.

- Most of the cybercrime victims are females between the ages of 20 and 30.
- Divorced women face more cybercrimes, especially sexual harassment
- The major causes of becoming a cybercrime victim are lack of internet knowledge and less use of internet security measures.
- There are other reasons for cybercrime victimization, which includes a lack of well-defined laws and regulations against cyber criminals.
- Fewer security measures are utilized by females using social apps such as Facebook and Twitter accounts, due to a lack of awareness about the potential risks.
- More time spent on social networking sites increases the chance of cyber victimization, such as cyber bullying and online harassment.
- Students are not using updated antivirus and security software because they do not know the importance of this software.
- Most of the women who are victims of cybercrimes do not report it to relevant agencies because they feel ashamed. They also lack confidence in the efficiency and procedures of these agencies.
- Women active in cyberspace confront different types of cybercrime exploitation than men. For example, they must cope with unsanctioned photograph circulation, anonymous phone calls of a profane nature, web-based hacking and abuse, counterfeit profiles, maligning, undermining calls, pantomime by hacking, provocation, transforming, phishing emails, stalking, online harassments, and more.
- As compared to married women, single women spent more time on the internet, and reported more friends on social

media websites. These factors are associated with increased risk of becoming victims of cybercrime.

- Regardless of their class standing, respondents are spending the same amount of time on the internet.
- Most of the time, the internet is accessed by phones, which are not a safe method of accessing private information such as bank accounts, and therefore increase the chances that information may be hacked.

Proposed Policy Updates

It is clear from the contextual evidence in this study that the current cybercrime prevention measures being practiced in Pakistan under the "Prevention of Electronic Crime Act of 2016" need updating and expanding. This act was quite comprehensive as laid out on paper, and covered all known domains of cybercrimes. But this law has also been called controversial, and criticized for ambiguity in many blogs and research articles (Arshad Khan, 2018; Khan, 2016). The reasons for this may be due to the lack of confidentiality for women reporting victimization, and also the impracticality of the penalties presented in the law. Thus, after detailed study on this serious issue, it became clear to me that there is a need to devise a policy which is easy to implement and uses strict confidentiality for those reporting, in order to seek justice for victims. Devising a public policy requires the support of public policy theory, as policy making never happens in a vacuum (Kitschelt, 1986). As per the concern of this study, discussion of the findings has its roots in system theory, because system theory includes the laws, rules and regulations, judicial decisions and the creation of pertinent legislation.

The issue of cybercrime victimization is a societal problem, affecting the public in a negative way. Thus, it is suggested that there should be a cybercrime unit in each police station, for collecting reports of cybercrimes and examining cybercrimes at the point of contact, as well as through home visits to respondents. Most of the women victimized strongly recommended that more female officers should be part of cybercrime units, because they believed that the presence of female officers may encourage more women to come forward and air their grievances without fear of additional exploitation. The FIA and police cyber units must collaborate with each other in order to increase the education and awareness of police cyber units on this topic. Most importantly, the confidentiality of the victim must be given the highest priority to protect their sense of self-worth. The penalties for harassers and cyber terrorists must be practical to enforce, and prison time must be ensured without bail.

Recommendations

The recommendations of this study are based upon the proposed policy and key findings already presented in this study.

- Cybercrime information must be a part of the curriculum in high school and in all college levels.
- A variety of classes and seminars must be arranged in order to create the awareness about cybercrime
- There should be a mandatory cybercrime unit in each police station, weighted with more female staff, in order to create a safe environment doe reporting and analyzing cyber crimes
- Law enforcement agencies should empower all police officers to respond sensitively to cybercrime complaints by offering essential education, public education can be accomplished through public service announcements via the web and the media transmission administrations, with the goal that all citizens will have essential knowledge of the types and impacts of cybercrimes. Officers who are managing cybercrimes need periodic classes and field training to maintain and update responses to cybercrime. Additional and on-going research is also important in order to stay abreast of changes in the types and relative frequency of cybercrimes, as well as the efficacy of education and the reporting process.

LITERATURE

Abrams, L.S. (2010). Sampling 'Hard to Reach'Populations in Qualitative Research: The Case of Incarcerated Youth. *Qualitative Social Work*, *9*(4), 536-550.

Al-Jazeera. (2016). *Cyber Harassment in Pakistan. How women are fighting back.* The Stream. Digital Rights Foundation

Alvi, M. H. (2016). *A Manual for Selecting sampling techniques in research*. Munich: Munich Personal RePEc Archive.

Anderson, J. & Rainie, L. (2018). The future of well-being in a tech-saturated world. *Pew Research Center*.

Andrews, D., Nonnecke, B., Preece, J. (2003). Electronic survey methodology: A case study in reaching hard to involve Internet Users. *International Journal of Human-Computer Interaction. 16*(2), 185-210.

Arfi, N., & Agarwal, S. (2014). Knowledge of cyber-crime among elderly across gender. *International Journal for Advance Research in Engineering and Technology*, *2*(2), 7-9.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis of the nature of groups engaged in cyber-crime. *An Analysis of the Nature of Groups engaged in Cyber Crime, International Journal of Cyber Criminology*, *8*(1), 1-20.

Bryan-Low, C. (2012). Hackers-for-hire are easy to find. *Wall Street J. 2012.*

Chao, C.M., & Yu, T.K. (2017). Associations among different internet access time, gender and cyberbullying behaviors in Taiwan's adolescents. *Frontiers in psychology*, *8*, 1104.

Churchill, G.A., Brown, T.J., & Suter, T.A. (1996). *Basic marketing research*. Orlando, FL: Dryden Press.

Crowther, G.A. (2017). National Defense and the Cyber Domain. *The Heritage Foundation*, 83-97.

Digital Rights Foundation. (2017). Cyber Harassment Helpline One-year Report December 2016 to November 2017. Retrieved September 29, 2020 from https://digitalrightsfoundation.pk/wp-content/uploads/2017/12/Helpline-Annual-Report.pdf

Donner, C.M. (2016). The gender gap and cybercrime: An examination of college students' online offending. *Victims & Offenders*, *11*(4), 556-577.

Duggan, M. (2014). Online Harassment. Pew Research Center: Internet. *Science and Tech. Available online: http://assets. pewresearch. org/wp-content/uploads/sites/14/2014/10/PI_ OnlineHarassment_, 72815*.

Gluschke, G., Hakki, M.C., Macori, M. & Leszczyna, R. (2018). Cyber security policies and critical infrastructure protection.

Federal Bureau of Investigation, Internet Crime Complaint Center. (2016). *Internet Crime Report 2016. Retrieved September 25, 2020 from:* fbi.org.

Gordon, S., & Ford, R. (2002). Cyber-terrorism?. *Computers & Security*, *21*(7), 636-647.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13-20.

Sheikh, H. (2013). Pakistan internet use survey 2013. *Express Tribune*.

Helweg-Larsen, K., Schütt, N., & Larsen, H.B. (2012). Predictors and protective factors for adolescent Internet victimization: Results from a 2008 nationwide Danish youth survey. *Acta Paediatrica*, *101*(5), 533-539.

Huff, R., Desilets, C., & Kane, J. (2010). *National public survey on white-collar crime.* Rockville: National White-Collar Crime Ctr.

Jamil, Z. (2006, August). Cyber Law. In *50th anniversary celebrations of the Supreme Court of Pakistan International Judicial Conference on* (pp. 11-14).

Jones, L.M., Mitchell, K.J., & Finkelhor, D. (2013). Online harassment in context: Trends from three youth internet safety surveys (2000, 2005,

2010). *Psychology of violence*, *3*(1), 53.

Peciuriene, J. (2017). Cyber violence is growing threat, especially for women and girls. News Article on topics Digital Agenda, Youth and Violence. Published on June 19, 2017. Retrieved September 25, 2020 from: https://eige.europa.eu/news/cyber-violence-growing-threat-especially-women-and-girls

Kemp, S. (2018). Digital in 2018: World's Internet Users Pass the 4 Billion Mark. January 30, 2018. Retrieved August 25, 2020 from: https://wearesocial.com/blog/2018/01/global-digital-report-2018

Khalil, B. (2020). Cybercrime effecting banking sector/ economy of Pakistan. Modern Diplomacy. Published in March 22, 2020. Retrieved September 26, 2020, from: https://moderndiplomacy.eu/2020/03/22/cybercrime-effecting-banking-sector-economy-of-pakistan/

Arshad Khan, E. (2018). The Prevention of Electronic Crimes Act 2016: An Analysis. *LUMS LJ*, *5*, 117.

Kitschelt, H. (1986). Four theories of public policy making and fast breeder reactor development. *International Organization*, *40*(1), 65-104.

Krejcie, R.V., & Morgan, D.W. (1970). Determining sample size for research activities. *Educational and psychological measurement*, *30*(3), 607-610.

Lavigne, C. (2008). *Mirrorshade Women: Feminism and Cyberpunk at the Turn of the Twenty-first Century*. Doctoral dissertation, McGill University, Montreal, Canada.

Lewis, J. (2018). *Economic Impact of Cybercrime, No Slowing Down*. McAfee.

Malik, M.A. (2018). *Preventing Cybercrime: A Criminological Perspective*. Islamabad: Center for Global & Strategic Studies.

McGuire, M., & Dowling, S. (2013). Cyber-crime: A review of the evidence. Summary of key findings and implications. *Home Office Research report*, *75*.

Mendes, K., Ringrose, J., & Keller, J. (2019). *Digital feminist activism: Girls and women fight back against rape culture*. Oxford: Oxford University Press.

Mohajan, H.K. (2017). Two criteria for good measurements in research: Validity and reliability. *Annals of Spiru Haret University. Economic Series*, *17*(4), 59-82.

Morgan, R.E., & Kena, G. (2017). Criminal victimization, 2016. *Bureau of Justice Statistics. NCJ*, *251150*.

Morgan, S. (2017). Cybercrime Report, 2017. Retrieved September 30, 2020 from: https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

Navneet, K. (2018). INTRODUCTION OF CYBER CRIME AND ITS TYPE. *IRJCS:: International Research Journal of Computer Science*, *5*(8), 435-439.

Nurse, J.R. (2018). Cybercrime and you: How criminals attack and the human factors that they seek to exploit. *arXiv preprint arXiv:1811.06624*.

Oksanen, A., & Keipi, T. (2013). "Young people as victims of crime on the internet: A population-based study in Finland." *Vulnerable children and youth studies*, *8*(4), 298-309.

Porche, I.R. (2019). *Fighting and Winning the Undeclared Cyberwar*. The Rand Blog. June 24. 2019. https://www.rand.org/blog/2019/06/fighting-and-winning-the-undeclared-cyber-war.html

Poulsen, K.P. (2018). The Decades' 10 most dastardly cybercrimes. Retrieved August 25, 2020 from: https://www.wired.com/2009/12/ye-cybercrimes/

Qarar, S. (2018). *Cybercrime reports hit a record high in 2018: FIA*. Dawn news report 23rd Oct, 2018. https://www.dawn.com/news/1440854

Khan, R. (2016). *Controversial cyber-crime bill approved by NA*. Dawn.

Remenyi, D., Williams, B., Money, A., & Swartz, E. (1998). *Doing research in business and management: an introduction to process and method*. London: Sage Publications.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students*. London: Pearson education.

Smith, R.G. (2010). Identity theft and fraud. *Handbook of internet crime*, 273-301.London: Routledge.

Smith, R.G., Cheung, R.C.C., & Lau, L.Y.C. (2015). *Introduction: Cyber-crime Risks and Responses—Eastern and Western Perspectives.* In Cyber-crime Risks and Responses (pp. 1-9). London: Palgrave Macmillan.

Statista, A. (2018). Number of monthly active Facebook users worldwide as of 1st quarter 2018 (in millions). *www. statista. com*.

Usman, M. (2016). *Cyber Crimes: A case study of legislation in Pakistan in the light of jurisdiction.* A dissertation to fulfill the corporate law degree. International Islamic University Islamabad, Pakistan.

Van de Weijer, S.G., & Leukfeldt, E.R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), 407-412.

Van de Weijer, S.G., Leukfeldt, R., & Bernasco, W. (2019). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology*, *16*(4), 486-508.

Waghole, S.N. (2019). Cyber Crime Statistics. *Journal of the Gujarat Research Society*, *21*(14s), 518-523.

Waldo, J., Lin, H.S. & privacy and information technology in a digital age: Executive summary. *Journal of Privacy and Confidentiality*, *2*(1). 5-18.

Zeviar-Geese, G. (2005). The state of the law on cyber jurisdiction and cybercrime on the internet. *In: California Pacific School of Law. Gonzaga Journal of International Law, 1*, 1997-1998.