IUB Journal of Social Sciences
https://journals.iub.edu.pk/index.php/jss
Vol. 3, No. 2, December 2021, Pages: 40-45

Causes and Effects of Cyber-Crime Victimization among Educated Youth: A Study of BZU, Multan

Aisha Khan[1], Sonia Akram[2], Saima Munir[3] and Iqra Almas[4]

Abstract

As criminal activities are increasing in Pakistan, there are different types of crime that come into the mind. Cyber-crime is the most common among internet users, especially students who are connected online most of the time for different purposes. This study examined the nature of cyber-crime, causes of cyber-crime its and effects on victims. The sample for the study consists of 201 students from department of social sciences Bahauddin Zakirya University, Multan. The researcher used multi stage sampling and questionnaires as a tool for data collection. The results were analyzed by using SPSS. The results revealed that 86.5% of the respondents used internet every day, while 95(47.2%) of respondents used internet for study, other 30(14.9%) heard songs by using internet, 45(22.3%) youth played games and 41(20.3%) watched movies. University students become victimized due to fake online job 124(61.6%), while monetary reward 37(18.6%), chat in open room 20(9.9%) and downloaded games 20(9.95%). There are different effects like 80(39.8%) psychological losses which include mental effect of private information losing and risk of re-victimization. While 55(27.3%) respondents are harassed, on the other hand 21(10.4%) respondents lost their financial data and 45(22.3%) students lost their personal information data. Future researches will be needed to let the youth be fully aware about cyber-crime effects.

Keywords*:* Cyber-crime, causes, effects, students, victimized, psychological loss, harass

1 Introduction

The emergence of computer and rapid growth of information technology have brought enormous benefits to modern society. The Internet in Pakistan has been available since the early 1990s and it has about 76.38 million internet users. Information and communications technology (ICT) is one of the fastest growing industries in the country. Information Technology is literally in every field of life now so in every achievement IT has definitely played a vital role. Information Technology is a growing and rising industry in Pakistan. The IT industry regarded

[1]Assistant Professor and chairperson, Department of Sociology, The Women University Multan, Pakistan. Email: aisha_aaur@yahoo.com
[2] M.phill Scholar, Bahauddin Zakirya University, Pakistan. Email: soniaakram392@gmail.com (co-responding author)
[3] Lecturer, Department of Sociology, The Women University Multan, Pakistan. Email: saimamunir018@gmail.com
[4] M.Phil. Scholar at Institute of Social Sciences, Bahauddin Zakariya University, Pakistan. Email: iqra.almas40@yahoo.com

as a successful sector of Pakistan economically, even in financial crisis. Information technology provide various opportunities to students for study it connected them globally. The internet enables them to share information and knowledge globally. Students go online for study, business, fun and entertainment. Although having a brighter side, there is a dark face of the internet as well that not everyone is aware of that. People can easily fall a pray to cyber-crime easily not knowing much about it. Even being fully aware of that some individuals would be victims of cyber-crimes one way or another on different levels.

Criminology is a branch of sociology that studies about different types of crime. In modern age the type and pattern of crime have changed. Criminal activities are expanding globally with the rapid use of digital technology. The expansion of computer connectivity increase risks to data privacy, setting new modes of criminal opportunity. The threat of cyber-crime and the capacity to respond to it will vary dramatically across nations (Baskerville, R., 1991).

The young generation is more sensitive and appears to have curiosity about everything. Cyber-crime is one of the major crimes and university students used internet for study, entertainment and fun therefore, getting chance of cyber-crime. Cyber-crime is generally described as a general term that refers to all criminal activities done using the means of computers, the internet, cyber space and the worldwide web. In other words, it is a crime in which a computer and its connected is the target of the crime being used as a tool to commit an offense.

Some of the kinds of Cyber-criminals are mentioned as: **Crackers:** These individuals are intent on causing loss to satisfy some antisocial motives or just for fun. Many computer virus creators and distributors fall into this category. **Hackers:** These individuals explore others' computer systems for education, out of curiosity, or to compete with their peers. They may be attempting to gain the use of a more powerful computer, gain respect from fellow hackers, build a reputation, or gain acceptance as an expert without formal education. **Pranksters:** These individuals perpetrate tricks on others. They generally do not intend any particular or long lasting harm. **Career criminals:** These individuals earn part or all of their income from crime, although they Malcontents, addicts, and irrational and incompetent people: In some cases they conspire with others or work within organized gangs such as the Mafia (Bowen &Mace 2009).

Cyber-crime in Asia as elsewhere may be caused by offenders or loose groups who are hacking “for fun” or ego driven, but can include political or ideological motivation, hatred, or simply to earn a profit. However the involvement of traditional criminal groups or new criminal networks is likely to be associated with financial deception and theft (Broadhurst and Choo 2011). In the current online era of cyber threats, a huge number of cyber threats and its impact along with understanding is difficult to restrict at the initial stage of the cyber-attacks. (Hale, C. 2002).

Cyber-crimes can be committed in a variety of ways such as a denial of service, stealing information, data diddling, email bombs, illegally getting access to computers or networks, virus attacks, stealing internet time, website hacking, Trojan attacks, pornography of children, violation of privacy, stealing intellectual property, spamming, phishing, terrorism through cyber media, piracy, cheating, fraud, drug trafficking or selling banned items and hacking, etc. Such crimes are committed for greed, fame, revenge, adventure, power, negative mindsets, etc. (Al-Hamami & Al-Sadoon, 2014).

Internet criminals can easily guess your passwords today because people are sharing their personal information over social networking websites. It can cause significant financial problems especially our banking system when almost every market is set online today. Regarding the cyber-crime, things can worsen even and result in physical harm. Interaction over the internet is no substitute for a warm handshake (Trout, 2007). The Internet, if properly exploited, is the modern business tool and financial management resource. In case of a cyber-attack, there will be no one today who will stay safe. The slow law enforcement is the actual problem that needs attention (Vazquez, 2006).

The objectives of the study as following:

1. To understand the nature of cybercrime.
2. To find out the causes of cyber-crime among university students.
3. To analyze the effect of cyber-crime among university students.

2 Materials and Methods

It was a quantitative research. Survey method was used to conduct the study and questionnaires were designed for data collection form the student to know their online social life, fear of cybercrime victimization, cyber-crime victimization causes and effects. The sample of the study was 201 students of BS and Master of BZU, Multan. The data was analyzed by using SPSS, getting frequency distribution and their causal relationship.

3 Findings & Analysis

Socio-demographic profile:

Some demographic characteristics of respondent study in this research are their Gender, education, age and residential area.

Table 1
Socio-demographic Characteristics of Respondent Regarding Gender

Variable	Category	Frequency	Percentage
Gender	Male	80	39.8%
	Female	121	60.2%

There were 121(60.2 %) of the respondents that were female students, found out during the research and80 (39.8%) of respondents were male students. This clearly depicts that female students were in higher ratio that the male students taken in this study.

Table 2
Socio-demographic characteristics of respondent regarding Education

Variable	Category	Frequency	Percentage
Education	BS	109	52.2%
	Master	92	45.8%

There were 109 (54.2%)of respondents that were BS students as depicted by the research study while 92(45.8%) of the respondents were Master degree students involved in the study.

Table 3
Socio-demographic characteristics of respondent regarding Age

Variable	Category	Frequency	Percentage
Age	17 to 21	101	50.2%
	22 to 26	96	47.8%
	27 to 31	4	2.0%

101(50.2%) of the respondents belonged to 17 to 21 year old age group96 ,(47.8%)respondents were from 22 to 26 year old age group and 4(2%)of the respondents age category was 27 to 31 year old.

Table 4
Socio-demographic characteristics of respondent regarding Residential Area

Variable	Category	Frequency	Percentage
Residential area	Rural	90	44.8%
	Urban	111	55.2%

44.8% respondents belonged to rural area as shown by the calculated results from the survey, while 55.2% respondents lived in urban area.

Table 5
Daily use of internet by the respondents

Daily use of internet	Frequency	Percentage
Yes	174	86.5%
No	27	13.6%
Total	201	100.0

Students use internet on daily basis for various purposes. They use it for getting information, fun and entertainment. Our results revealed above that majority 174(86.5%) respondents use internet on daily basis while 27(13.6%) do not use it on every day basis.

Table 6
Purposes of use internet

Category	Frequency	Percentage
Study Materials	95	47.2%
Hearing songs	30	14.9%
Sports and game	45	22.3%
Movie	41	20.3%
Total	201	100.0

The data collected as above shows that 95(47.2%) of participants use internet for study related purposes, 30(14.9%) individuals us it for listening to music , on the other hand 45(22.3%) individuals played games through it and 41(20.3%) number of students watch movies while using internet.

Table 7
Causes of cyber-crime victimization

Category	Frequency	Percentage
Fake online jobs	124	61.6%
Trap of monetary reward	37	18.6%
Chat in open room	20	9.9%
Game download	20	9.9%
Total	201	100.0

The above data shows that 124(61.6%) respondents become victimized due to fake online job, while monetary reward affected 37(18.6%) individuals, chat in open room involved 20(9.9%) participants and game downloading individuals ratio was 20(9.9%).

Table 8
Effects of cyber-crime victimization on respondents

Category	Frequency	Percentage
Psychological losses	80	39.8%
Harrasment	55	27.3%
Financial loss	21	10.4%
Personal data loss	45	22.3%
Total	201	100.0

Primary victimization contains psychological losses to 80(39.8%) students. It depicts the mental effect of private information loss and risk of re-victimization. While 55(27.3%) respondents were harassed somehow while using internet. On the other hand 21(10.4%) students lost their financial data and 45(22.3%) students lost their personal data.

4 Conclusion

While using the internet, cyber-crime showed a peak in female students involved in the study. Also from age 17 to 21 and 22 to 26 were in majority for having faced cyber-crime having different effects on them. Users faced cyber-crime by trusting fake online jobs was in a higher ratio. Psychological loss was the number one effect on the users facing cyber-crime. Using the internet without proper security and verification improves Internet harassment, hacking and also various other criminal activities that one can face without having much knowledge about it. In order to digitalize our country, there is no alternative to secure technology. Internet using should prevail in priority but it must be heavily secured and safe for everyone's use. Along with raising awareness the law enforcement agencies and all stakeholders have to walk together to curve the modern perils like cyber-crime.

References

Al-Hamami, A. H., & Al-Sadoon, G. M. (2014). Handbook of Research on Threat Detection and Coutermeasures in Network Security: Advances in Information Security, Privacy and Ethics. Hersley: IGI Global.

Baskerville, R. (1991). Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security, European Journal of Information Systems, 1 (2): 121-130.

Bowen, Mace (2009). Computer Crime, Available at: http://www.guru.net/, Visited: 28/01/2012

Broadhurst, R., & Chang, L. Y. (2013). Cybercrime in Asia: trends and challenges. In *Handbook of Asian criminology* (pp. 49-63). Springer, New York, NY.

Hale, C. (2002). Cybercrime: Facts & figures concerning this global dilemma. Crime and Justice International, 18(65), 5-6.

Trout, B. J. (2007). *Cyber law: A legal arsenal for online business*. World Audience Inc.

Vazquez, C. I. (2006), Cyber crime the internet and its impact on the business enterprise and the role of the technology manager. *Capstone Project*, University of Denver.