International Journal of Asian Social Science
ISSN(e): 2224-4441/ISSN(p): 2226-5139
journal homepage: http://www.aessweb.com/journals/5007

AWARENESS REGARDING CYBER VICTIMIZATION AMONG STUDENTS OF UNIVERSITY OF SINDH, JAMSHORO

Muhammad Abdullah Avais[†]
M.Phil Scholar, Department of Sociology, University of Sindh, Jamshoro
Aijaz Ali Wassan
Associate Professor, Department of Sociology, University of Sindh-Jamshoro
Hameeda Narejo
Lecturer, Department of Sociology, University of Sindh Jamshoro
Jameel Ahmed Khan
M.Phil Scholar, Department of Sociology, University of Sindh, Jamshoro

ABSTRACT

The crimes that are committed by computers and networks called cybercrimes. The aim of study is to know the awareness towards cyber victimization among students of university of Sindh Jamshoro. 100 students (50% male and female) were selected through purposive sampling. The result shows that 77% respondents don't bother to share their personal informations with cyber friends. Only 41 % respondents like to read policy guidelines of any social networking site. 57 % respondents use internet more than 06 hours on daily basis. 82% respondents believe that women are more prone to cyber attacks. 73% respondents don't know regarding any government department for their help in case of cyber victimization.

Keywords: Cybercrimes, Social networking, Awareness, Students, University of Sindh, Jamshoro.

Contribution/ Originality

This study is one of very few studies which have investigated awareness level of students regarding cyber victimization, and trend of usage of social networking sites in context of University of Sindh, Jamshoro. The result of study shows that government as well as social sector must conduct a survey on broad base. It explores new ways for policy makers.

† Corresponding author
ISSN(e): 2224-4441/ISSN(p): 2226-5139

1. INTRODUCTION

In Pakistan, cyber crimes are new and complicated curse. (Cyber-Crime) encompasses any criminal act dealing with computers and networks (Wired or wireless) (Cyber-Crime). Due to lack of knowledge regarding laws that address cyber crimes in Pakistan and victims' rights most of people don't report to authorities. Millions of people are regular internet users in Pakistan who are frequently part of cyber space due to their professional, personal needs or for education purpose. Pakistan has no exclusive legislation dedicated for information technology compare to India.

It is alarming that due to unawareness rate of E-victimization is increasing. E-Victimization is the type of victimization that is not occurred face to face. It occurred through computer or other electronic devices or software. This may took place to intentionally harm the reputation of victim or group. Cybercriminal are similar with traditional criminals. The aim of Cyber criminals to earn money as quickly and easy as possible and the same phenomena we study in traditional criminals (Kunz and Wilson, 2004). We try to save our houses, buildings and offices to equip them with technical checks (CCTV, Alarms etc). Similarly we can prevent ourselves in cyberspace with help of little technical education and common sense. In Pakistan a department with name of "(National Response Center for Cyber Crimes) (NR3C)" under the umbrella of Federal Investigation Agency (FIA) is functional but awareness towards NR3C is a mark able question.

1.1. Demographic of Jamshoro

Jamshoro is commonly known as "City of Knowledge" due to 03 biggest universities (1. University of Sindh, 2. Mehran University of Engineering and Technology (MUET) & 3 Liaquat University of Medical Health & Sciences (LUMHS)). It was bifurcated as district in 2004 from district Dadu. It is consisted on 03 taulkas and its total geographical area of the district is 11,517 square kilometers (The Brief District Jamshoro, 2004) and its literacy rate is 43.6% (Demography of Jamshoro).

1.2. Historical Background

In history first cyber crime was recorded in 1820 in France (Kabay, 2008). In 1960-1970 computer crimes were involved physical damage to computer system and subversion of the long-distance telephone networks (Kabay, 2008).

1.3. Literature Review

Matthews (2010) argues that any crime that involves computer or computer network is called cyber crime. Any crime where is possibility that computer may play an important role is called cybercrime (Thomas and Loader, 2000). A new generated theory regarding (Cyber-Crime) is "Space Transition that was developed by Dr. Jai Shankar (Jaishankar, 2008). It argues that behavior of people is different when they move from one space to another space. It theorizes that "1. Persons, due to their status and position cannot commit crimes in physical space have tendency to commit crime in cyber space. 2. Due to lack of deterrence factor, flexibility in identity factor, cyberspace provides the choice to offender to commit (Cyber-Crime) 3. In Cyberspace, behavior of offender is likely to be imported to physical space. 4. Intermittent ventures of offenders in to the

cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape 5. (A). Cyberspace may lead to unite strangers in physical space to commit crimes. (B). A group of people having common purpose or interest in Physical space may likely to unite to commit crimes in cyberspace. 6. Persons belonging to closed society are more likely to commit crimes than belonging to open society in cyber space. 7. Norms and values of both cyber and physical space may lead to (Cyber-Crime).

1.4. Objectives of Study

1. To find out the way of individual victimization.
2. To analyze the respondents knowledge regarding cyberspace victimization.
3. To examine the respondents knowledge regarding anti (Cyber-Crime) acts.

1.5. Research Methodology

It is an exploratory research with quantitative analysis through interview schedules. In 2010 a baseline survey was conducted in India on cyber victimization (Debarati and Jaishankar, 2010). Researcher used the questioner of baseline after necessary amendments in context of Pakistan for current study. A sample of 100 respondents (B: 50 & G: 50) through purposive sampling from various departments of University of Sindh Jamshoro were selected. All respondents were computer literate and used to spend minimum 02 hours daily on social networking sites. The age of respondents were vary due to their session years but all samples were belonged to 18 to 24 years age.

1.6. Limitations

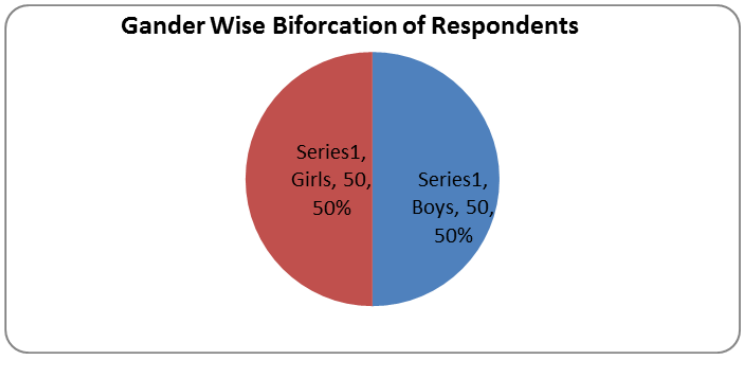
This study was conducted to analyze the awareness toward Cyber Victimization among Students of University of Sindh, Jamshoro. The ongoing study covers only one university. There is highly need to conduct this survey on broader base.

1.7. Results & Discussions

1.7.1. Background of Study

1. Respondent's background is as under:-

Graph I



Analyses: Graph I is showing that 100 respondents (B: 50 & G: 50) were selected from University.

2. AWARENESS OF (CYBER CULTURE)

Table-1.

Awareness among (Cyber Culture)	Yes %	No %
Do you know regarding minimum age to join cyber community as like Facebook etc?	86	14
Do you allow others (Friends, relatives) to use your personal ID?	31	69
Do you use safety tips like filtering emails, password seal to protect your ID?	61	39
Do you mail back to unknown senders of spam mails?	29	71
Do you share personal information / emotions with virtual friends /chat room partners etc whom you don't know in real life?	77	23
Do you believe in controlling free speech while communicating in the cyberspace?	54	46
Do you read policy guidelines of social networking sites before Joining?	41	59
Do you use nick names on profiles instead of real names?	53	47

Source: Primary Data

Analyses: Graph 1 is showing the respondents awareness regarding (Cyber Culture). The dictionary of Oxford (Cyber Culture) is defining it as "the social conditions brought about by the widespread use of computer networks for communication, entertainment, and business: *our lives are influenced by (Cyber Culture).* The (Cyber Culture) may be defined in technical term that, 1. To know the minimum age, that is required for entrance in cyber community, 2. How to use their right "(Freedom of Speech)", 3. Activities that are involved with personal information sharing[13].

2.1. Minimum Age

The result is showing that 86% respondents are aware regarding minimum age that is essential to join cyber community/social site etc. While 14% respondents are not aware regarding minimum age to join cyber space.

2.2. Allow Other to Use Personal ID

All the respondents are student of university and it is very alarming that 31% respondents replied that they allow others (Friends) to use their personal ID and password. It is more alarming when we see that 86% respondents know the minimum age to join cyber space and other hand 31% respondents allow to their friends, relatives to use their own id and password to chat with others or mail them.

2.3. Safety Measurements

61% respondents are aware regarding safety measures or self protection tools. Either they know it after any incident, friend or through available internet material. The respondents use internet filtering, block obnoxious person, locked personal walls, albums or friend lists etc. While 39% respondents are not aware regarding these methods or they don't like to use.

2.4. Mail Back

29% respondents replied that they are used to mail back to unknown person while 71% respondents said that they don't like to reply on mail of unknown sender.

2.5. Share Personal Information

77% respondents are used to share original information likewise contact numbers, age, addresses or personal feelings. They share their personal information with which they have never seen in real world or they know only on cyber space. While 23% respondents share their personal information with only known persons.

2.6. Free Speech

54% respondents feel that there must be control on free speech. These respondents belong to Pakistan and they are used to use chat rooms or other social networking sites like facebook, orkut etc. These sites are being operated by US law of "(Freedom of Speech) while in Pakistan, the meaning of (Freedom of Speech) is different. Article 19 of constitution of Pakistan 1973 describes it as "*Every citizen shall have the right to freedom of speech and expression, and there shall be freedom of the press, subject to any reasonable restrictions imposed by law in the interest of the glory of Islam or the integrity, security or defense of Pakistan or any part thereof, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, 1[commission of] or incitement to an offence* (Freedom of Speech, 1973). The concept of (Freedom of Speech) under US law is "*Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the (Freedom of Speech) or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances (1st Amendment).*" 46 % respondents believe that there is neither need to control on (Freedom of Speech) nor amendments.

2.6. Reading Policy Guidelines

The policy guidelines of various cyber communities are very important source to develop (Cyber Culture). Most of social networking sites use their own policy guidelines to develop it. The aim of these guidelines to prevent their users from, hacking and its related issues, e-crimes, sexual crimes, child abuse and pornography. Sometime these communities don't believe in to protect religious thoughts. For example in Pakistan "Youtube" is banned from last many years due to availability of hate material against prophet "Muhammad (PBUH). 41% respondents read the policy guidelines of social communities before entering and 59% respondents do not read policy guidelines

2.8. Nick Names

53% respondents admit that they use Nick (Pseudo) names on cyber space. A pseudo name, that a person or group use for specific purpose and it is different form his/her real name (Pseudonym, 2013). Therefore the meaning to use these names may be to protect their identity. 47% respondents don't use nick names.

3. FREQUENCY IN CYBER NETWORKING

Under this part we will study the frequency level of respondents towards on line activities.

Table-2.

Frequency in (Cyber Culture)	High% (> 06 hours)	Moderate %(03-05 hours)	Low % (< 02 hours)
How many time you spend in cyber space	57	39	4
Frequency in the chat rooms	49	37	14
Frequency in interacting with unknown chat partners	37	53	10

Results

The table 2 is showing that 57% respondents are highly active on internet. They use more than 06 hours on various social networking sites. 39% respondents spend 03-05 hours and 4% respondents spend below than 02 hours on social networking sites. Most of the respondents are belonging to high and moderate category. 49% respondents are highly active in chat rooms, 37% respondents are on high risk of victimization due to interaction with unknown persons in cyber communities. 37% respondents spend 03-05 hours and 14% minimum 02 hours daily in chat rooms. 53% respondents interact with unknown persons in chat room.

4. KNOWLEDGE OF VICTIMIZATION

In this part we will analyze the respondent's knowledge toward their victimization and their knowledge to its reporting mechanism

Table-3.

Knowledge of Victimization	Yes%	No%	Don't Know %
Did you ever face bad experience in the social networking sites?	69	27	4
Did you ever receive abusive / dirty mails in inboxes from known / unknown sources?	73	27	0
Did you ever experience of hacking (either directly /indirectly) your ID	37	52	11
Did you ever face/experience cyber stalking?	23	60	17
Did you feel that you were victim of phishing attacks?	46	44	10
Did you ever see you are impersonated by email account /social networking profiles /websites etc?	29	70	1
Did you ever see you're cloned' profile/email ids?	47	50	3
Do you feel that you are a victim of defamatory statements/activities involving yourself in the cyber space?	59	39	2
Did you ever receive hate messages in your inboxes/message boards	65	30	5
Did you ever see your morphed picture on cyber space?	36	60	4
Did you ever been bullied?	40	47	13

Continue

Did you ever face experience of flaming words from others?	60	36	4
Did you ever Victimized by your own virtual friends?	33	60	7
Did you report your bad experience to authorities?	25	47	28
Do you feel that women are prone to cyber attacks?	82	18	
Is there any government department to control on cyber victimization in Pakistan	17	73	10

Source: Primary Data

Results

4.1. Hacking/Stalking/Phishing etc

Table III is showing that 37% respondents have faced victimization of hacking in different ways like, email id, facebook account etc. 52% respondents are never hacked as they continuously upgrade their system or take precautionary measures. 11 % respondents are not aware weather they were hacked or their account is hacked. 23% respondents feel they have faced cyber stalking. Cyber stalking has same characteristics as traditional stalking but it occurs through internet. 60 % respondents have not experience of cyber stalking and 17 % respondents are not aware weather they were stalked or not. 46% respondents suffered through phishing attacks. The common method of attack to get personal information like, name, date of birth, credit card number or bank account etc. People receive a fake mail with id of "Yahoo", "Gmail" or any bank in which they forced to share these information otherwise their account will be closed. 44 % respondents did not face this attack because they never replied to these mails or they know about these mails and they treat these mails as spam. 10 % respondents are not aware regarding these type of phishing mails.

4.2. Impersonation

29 % respondents are aware of being victimized by impersonated profiles. The meaning of impersonate is to pretend to be someone you are not: something with fraudulent intentions. Impersonate profiles are fake profiles that were made by any individual or group with help of screen name and personal information and some time picture or picture id of someone to cheat others or damage the personality of account holder. 70 % respondents did not face this attempt and rest of respondents do not know regarding impersonation.

4.3. Defamatory, Bullying, Flaming and Hate Messages

59 % respondents faced defamatory statement through emails or in chat rooms or in community discussions. 28% did not seen such messages and 02 % do not know regarding defamatory statements. 40 % respondents received bullying messages 60 % received flaming words either through mails or in public/private chat groups. 36 % respondents saw their morphed pictures. 36 % did not received flaming words and 04 % respondents do not know regarding this. 60 % respondents never seen their morphed pictures.

4.4. Victimization through Cyber Friends

33 % respondents feel that they were victimized by their virtual friends. 60 % respondents informed that they were never victimized. 07 % respondents do not know regarding their victimization. It shows that the people who dislike to chat with unknown persons or don't reply to unknown emails are less like to be victimized.

4.5. Reporting

Only 25% respondents reported to authorities i.e facebook, gmail etc regarding cyber-attacks. 47% respondents did not report to anyone. 28% respondents don't know the reporting procedure.

4.6. Women Status

82% respondents felt that women are prone to cyber attack on internet while 18% respondents feel that there is no risk for cyber-attack on women.

4.7. Government Department in Pakistan

Results of study show that awareness regarding government department to control cyber crimes is very poor. Only 17% respondents know that a government department is working to control cyber crimes, 73% respondents believe that cyber crime control department don't exist and 10% respondents don't know either department exist or not.

5. AWARENESS TOWARDS LEGAL RIGHTS

In this part we will discuss, respondent's knowledge toward legal rights.

Table-4.

Awareness of Rights and Reporting Behavior	Yes%	No%
Do you know that hacking, creation of pornography/distributing the same, distribution obscene materials etc are criminal offences by the Law?	77	23
Do you know regarding your legal rights to protect privacy in the cyber space?	68	32
Do you know that cyber bullying, cyber stalking, sending annoying, defaming messages etc can be penalized?	27	73
Did you report such incidences of cyber victimization to concern authority (FIA)?	04	96

Source: Primary Data

Results

Electronic Transactions Ordinance (2002) was first anti (Cyber-Crime; Prevention of Electronic Crimes Ordinance, 2007) ordinance in Pakistan. In 2007 a new ordinance "(Prevention of Electronic Crimes Ordinance, 2007)" was introduced.

The table IV is showing the results of various questions. 77% respondents are aware that hacking, creation of pornography and its distribution is illegal and punishable offense.

68%respondents are aware regarding their rights on cyber space. 27% respondents are aware that bullying, stalking or defaming messages through cyber space are illegal and can be penalized. Only 04% respondents consulted with "Federal Investigation Agency" or its (Cyber-Crime) cell.

6. CONCLUSION

It is demanding of time to study cyber victimization on grass route level. The results are showing the importance of awareness as a method to decrease or prevent (Cyber-Crime). We can condemn unethical (Cyber Culture) with partnership and collaboration of both individuals and authorities. Government can do more to safe and secure cyber space. Although we cannot make free cyber space from attacks but it is possible to combat and check the (Cyber-Crime). To achieve this goal our first duty is to educate people regarding (Cyber-Crime) and precautions to prevent from it (Arpana and Meenal, 2012).

7. SUGGESTIONS

1. Government must be arranged an awareness campaign to educate the university students as well as schools and colleges about cyber ethics.
2. There is highly need from FIA to conduct awareness seminars in universities regarding cyber victimization, safety parameters and reporting mechanisms.
3. At university levels government or competent authority (HEC) must include courses for teachers regarding (Cyber-Crime).
4. Social sector (NGO) must participate and conduct awareness regarding cyber victimizations and work on rehabilitation of cyber victims.

REFERENCES

1st Amendment, US law of free speech. Available from http://topics.law.cornell.edu/constitution/first_amendment.

Arpana and C. Meenal, 2012. Preventing cyber crime: A study regarding awareness of cyber crime in Tricity. International Journal of Enterprise Computing and Business Systems, 2(1).

Cyber-Crime, In webopedia. The Free Online Technical Dictionary. Available from http://www.webopedia.com/TERM/C/cyber_crime.html.

Cyber Culture, In Oxford dictionary. The free online dictionary. Available from http://www.oxforddictionaries.com/definition/english/cyberculture [Accessed 10-03-2014].

Debarati, H. and K. Jaishankar, 2010. Cyber victimization in India: A baseline survey report Tirunelveli. India: Centre for Cyber Victim Counselling. Available from http://www.cybervictims.org/CCVCresearchreport2010.pdf. (Accessed on 10-03-2014).

Demography of Jamshoro, Thar deep rural organization. Demography of Jamshoro. Available from http://www.thardeep.org/thardeep/jamshoro.html.

Electronic Transactions Ordinance, 2002. Gazette of Pakistan, extraordinary, Part-I of 2002. Pakistan F. No. 2(1)/2002-pub. Available from http://www.fia.gov.pk/ETO.pdf [Accessed 10-03-2014].

Freedom of Speech, Constitution of the islamic republic of Pakistan. (1973). Pakistan. Available from http://pakistanconstitutionlaw.com/article-19-freedom-of-speech-etc/.

Freedom of Speech, 1973. Constitution of the islamic republic of pakistan. Pakistan. Available from http://pakistanconstitutionlaw.com/article-19-freedom-of-speech-etc/.

Jaishankar, K., 2008. Space transition theory of cyber crimes, crimes of the internet. Pearson Publishers. pp: 283-299.

Kabay, M.E., 2008. A brief history of computer crime. An introduction for students. School of Graduate Studies Norwich University SA. Available from http://www.mekabay.com/overviews/history.pdf [Accessed 10-03-2014].

Kunz, M. and P. Wilson, 2004. Computer crime and computer fraud. Professional Master Degree Thesis. Department of Criminology and Criminal Justice in University of Maryland.

Matthews, B., 2010. Computer crimes: Cybercrime information, facts and resources. Available from http://www.thefreeresource.com/computer-crimes-cybercrime-information-facts-and-resources [Accessed 10-03-2014].

National Response Center for Cyber Crimes, Introduction of NR3C. Available from http://www.nr3c.gov.pk/index.html.

Prevention of Electronic Crimes Ordinance, 2007. Gazette of Pakistan, extraordinary, Part-I of 2007. Pakistan.

Pseudonym, 2013. In wikipedia. The Free Encyclopedia. Available from http://en.wikipedia.org/wiki/Pseudonym.

The Brief District Jamshoro, 2004. Available from http://jamshoro.com.pk/Profile.htm.

Thomas, D. and B. Loader, 2000. Cybercrime: Law enforcement, security and surveillance in the information age. London: Routledge.