Social Sciences
2016; 5(1): 1-6
Published online March 4, 2016 (http://www.sciencepublishinggroup.com/j/ss)
doi: 10.11648/j.ss.20160501.11
ISSN: 2326-9863 (Print); ISSN: 2326-988X (Online)

Underlying Causes of Cyber-Criminality and Victimization: An Empirical Study on Students

Naznin Shabnam[1], Md. Omar Faruk[2], Md. Kamruzzaman[2, *]

[1]Department of Criminology, Faculty of Social Science, University of Dhaka, Dhaka, Bangladesh
[2]Department of Criminology and Police Science, Faculty of Life Science, Mawlana Bhashani Science and Technology University, Santosh, Tangail, Bangladesh

Email address:

shabnamnaznin@gmail.com (N. Shabnam), ru_faruk@yahoo.com (Md. O. Faruk), shohag.mbstu.cps@gmail.com (Md. Kamruzzaman)

To cite this article:

Naznin Shabnam, Md. Omar Faruk, Md. Kamruzzaman. Underlying Causes of Cyber-Criminality and Victimization: An Empirical Study on Students. *Social Sciences.* Vol. 5, No. 1, 2016, pp. 1-6. doi: 10.11648/j.ss.20160501.11

Abstract: In Bangladesh, like all other countries of the world the frequency of cyber-crime is increasing over the time. Generally, crime is defined by law as a territorial phenomenon in the way the law is territorial in nature. However, due to the global connectivity and online activities cyber crime has become a global matter, not a territorial one and is spreading in a terrific volume. Many of the students who study in the university level also without knowing the furiousness about the nature of cyber crime are being involved in such crime in various ways. This study therefore, is an effort to understand the involvement of students in cyber crime with or without their knowledge regarding the malicious sides of it. Mawlana Bhashani Science and Technology University was selected as the study area for the present study and a number of 175 undergraduate students have been interviewed during the time frame of June to October, 2014 to know their involvement as stakeholders in the same. This study has yielded some interesting findings about cyber criminality and victimization status of the students as like nature of victimization, way of victimization, victim offender relationships, types of cc, nature of cc criminal etc. Most of the studied respondents have a little or no knowledge regarding cyber crime and they are involved in such crime as offender just for mere interest and not for the illegal monetary gain; most of the respondents have also encountered one or many of the cyber crimes in their online activities. Psychological motivation is one of the main causes behind cyber-criminality of such youths and it is pertinent from the study that a very few of them is aware about the Information and Communication Technology (Amendment) Act, 2013 of Bangladesh.

Keywords: Cyber-Criminality, Causes, Victimization, Students

1. Introduction

Bangladesh is a developing country with a large number of populations in a small area. Targeting to make digital Bangladesh by 2021; people have already walked into the era by getting various facilities & scope on it. From the various scopes one of the greatest facilities is to study about modern technologies in public universities. Recently, there are some public universities based on science & technology opened their work [1]. Those have provided various modern technology based subject & to study them most amount students are interconnected with the PC/internet & starting an online lifestyle. The Internet has enabled us to share a marvelous amount of information and knowledge globally. Individuals go online for study, business, fun, and entertainment [2].

Since the 1990s, academics have observed how the cyber space has emerged as a new locus of criminal activity, but in general, criminology has been remiss in its research into the phenomena of cyber crime and has been slow to recognize the importance of cyber space in changing the nature and scope of offending and victimization. As such, very few theoretical explanations of cyber crime exist [3].

Criminology one of the branch of sociology always study about various types of crime but in modern era the pattern of crime is changed & also the pattern of criminal tendency is changed. Before this study of cc generally the student's victimization in public universities refers various types of violence as like political dominance, political empowerment, deviant behaviors etc. But they don't feature as a criminal until. Here the research purposed to define the criminogenic traits or students as a cyber victim because cc is an intellectual

crime & generally it is occurred in intelligence society [4].

The young generation generally sensitive & appear curiosity about any matter. Cyber crime is one kind of intellectual crime & the university student have a chance to use internet for their study & entertainment purposes & from that issues get that chance. Youth victimization history increases risk of involvement with delinquent peers and of subsequent delinquent behavior. A kind of role modeling effect takes place in the at-risk age years of 13-17, and when the person grows up past age 18, they become either a repeat victimizer or victim. Association with deviant peers and involvement with substance abuse increases risk of victimization. This study seeks to analyze the behaviors of university students, specifically by looking at where they are on the Internet, what their behaviors are on the Internet, and what they are doing to protect themselves while they are on the Internet [5].

Computer crime or cyber crime is a form of crime where the Internet or computers are used as a medium to commit crime. Criminogenic needs are factors in an offender's life that are directly related to recidivism. There are six factors that are directly related to crime: low self-control, anti-social personality, anti-social values, criminal peers, substance abuse and dysfunctional family [6].

Handling et al. (1978) suggest that an individual's daily patterned activities, such as vocational and leisure activities, contribute to victimization. They posit that an individual's expected social roles and social position influence their personal life style patterns, and contribute to the individual's decision to engage in certain activities. More importantly, engaging in risky activities can be made through individual rational choice.

Cohen and Felson (1979) assume that there are three main components to predict a likelihood of an occurring victimization event. First, a motivated offender must exist for the victimization to occur. Second, the presence of a suitable target is necessary for the occurrence of the victimization. Third, the absence of a capable guardian makes easy access for offenders to victimize the target [7]. There must be a confluence or convergence of all three components for the victimization to occur. Thus, absence of one of the three components is likely to decrease or eliminate the victimization occurrence.

When an online user accesses the Internet, personal information in his or her computer naturally carries valuable information into cyber space that attracts computer criminals. In addition, if computer criminals have sufficiently capable computer systems, the inertia of the crime target becomes almost weightless in cyber space. The nature of visibility and accessibility within the cyber-environmental so allows the motivated cyber-offenders to detect crime targets and commit offenses from anywhere in the world [8].

2. Objectives of the Study

The purposes of this study is to explain the nature, scopes & causes of cyber crime victimization & criminogenic traits of youth cyber user at public universities via specific components from traditional victimization theories (lifestyle-exposure theory and routine activities theory) at a micro level & the respondent's others nature of using pc/internet. This will be accomplished by examining the individual's online lifestyle, and measuring the presence of the actual installed computer security in their computer system.

The sections that follow will present an overview of lifestyle-exposure theory and the habit of pc/internet use of students and an overview of computer crime and victimization.

The study objectives of this research project refer-

i. To define the nature of cyber victimization
ii. To explain the causes of victimization of cyber user
iii. To understand the nature of cyber crime

3. Methodology

It was an exploratory research. Survey method was used to conduct the study while a semi-structured questioner was designed for interviewing the student to know their online social life, fear of cyber crime victimization, cyber crime victimization status & causes. A logical frame work was developed on the basis of various way data analysis such as frequency distribution, causal relationship, factor analysis &others statistical tools of univariet & bivariet analysis.

4. Findings & Analysis

Socio-demographic analysis:

In this research used some demographic characteristics of respondent to study their background & identify profile. Here used, Sex, age, marital status, religion, and those demographic characteristics.

Table 1. *Socio-demographic characteristics of respondent.*

Variable	Frequency
Gender	Female 26. 9%. And 73.1 % male.
Age	Age Range 18-25 years, Avg. age 22
Marital status	97.9% students were unmarried & only 2.1% was married
Religion	70.3% were Muslim, 29.1% Hindu &.06% Buddhist.

Measurement of self assessments by the personality traits-Introverts and Extroverts.

As researcher Arnold Henjum states "…studies provide evidence that there is a positive relationship between introversion and achievement. It seems likely that the introvert's vigilance or "stick to the task" accounts for a great deal of this success. Also, the introvert's self-sufficient, hard-working attitude and introspective, analytical style equips her/him very well for the demands of rigorous, abstract activities" (2001, page41). These comments corroborate similar observations put forth by famed personality theorist, Hans Eysenck. He concluded that introverts appear to possess a greater capacity for concentrated work which may translate into advantages in educational achievements (Eysenck, 1971).

It is not easy to identify what quality the respondents are. But if the respondents claim himself as extrovert or introvert

then it is so easy to define him according to his own point of view. Here to define respondent's psychology & personality traits on behalf their own opinion that simple answered helped to identify their victimization. Because when someone claims himself as extrovert then it can imagine that the person is extraordinary he may be involved a lot of work beside his profession & there is a little bit possibility to be a victim or he able to make many friend whose may fallen him victim or he have opportunity to do crime.

From this study findings 53.1% students think about as extrovert & 46.9% claim themselves as introvert personality. But if we compared it with passing period on pc we saw introvert people are involved highest period 9+hours per day & they have more possibility to be cyber victim or cyber criminal.

Table 2. *Self assessments of respondents.*

Respondents think himself		Frequencies	Percent
	Extrovert	93	53.1
	Introvert	82	46.9
	Total	175	100.0

Technical opportunities of respondents: Respondents used pc/internet daily

Beside the student of computer based subject others students also use pc/internet every day. Some student although they have no personal pc/internet connection. Again some student doesn't used pc/internet although they have personal pc/internet. Here from the total population of 175 about 54.9% people used pc/internet every day. That could be regarded as online lifestyle of respondents & according to RAT there is a possibility to be a victim of cyber crime.

Table 3. *Respondents as daily user of internet.*

Daily user of pc/internet		Frequencies	Percent
	Yes	96	54.9
	No	79	45.1
	Total	175	100.0

Purpose on use of pc/internet of respondents

As the world grows technology and people develop, new times bring new opportunity to learn easily. Computer is a new phenomenon sweeping the world as well as our academic field. The main purpose of used pc/internet of the student of public university but they also use it various purpose beside study. As like-Entertainment instrument, media of communication, sports & someone regard it as the best company.

Table 4. *Purposes of use pc/internet of respondents.*

Observe site	Frequencies	Percent
study materials	93	53.1
hearing song	12	6.9
sports & games	16	9.1
movie/natok	11	6.3
pornography/images	3	1.7
social side as facebook, yahoo messenger etc	5	2.9
None	35	20.0
Total	175	100.0

Table 4 presented that, about 93 respondents used pc/internet for study purpose from total population 175. And 9.14% played games, 6.8% hearing song, 6.29% see movie/natok, 2.9% enter in social side as facebook, yahoo messenger etc.

Victimization related analysis:

Internet use is drastically increasing and in turn, cyber space victimization is also on the rise. However, there are no studies to date that present a causal explanation of the relationship between youth online use and their victimization. The current study will seek to fill the gap in the literature by considering an explanation of cyber crime victimization based on Routine Activities Theory. An analysis of data collected from a survey of public university students.

Cyber crime knowledgeable Respondents:

The rapid development of technology is also increasing dependency on computer systems. Today, computer criminals are using this increased dependency as a significant opportunity to engage in illicit or delinquent behaviors. The concept of cyber crime is a new concept of criminology. It is almost impossible to have precise statistics on the number of computer crime and the monetary loss to victims because computer crimes are rarely detected by victims or reported to authorities. Then it is a matter of sorrow but true that there are many Student does not familiar with the concept of cyber crime although they have used pc/internet.

Table 5. *Cyber crime knowledgeable Respondents.*

Cyber crime knowledgeable		Frequencies	Percent
	Yes	65	37.1
	No	110	62.9
	Total	175	100.0

Table 5 reveals only 37.1% students are familiar with the concept of cyber crime**.**

Fear of crime of the respondents

The fear of crime refers to the fear of being a victim of crime as opposed to the actual probability of being a victim of crime. The core aspect of fear of crime is the range of emotions that is provoked in citizens by the possibility of victimization. Fear of crime makes people feel vulnerable & isolated, it reduces a person general sense of well being, and it motivates people to take crime presentation al techniques [9]. Here found that although they have no introduce about the concept of cyber crime but they have more fear of crime. About 63% of total populations have fear of cyber crime.

Table 6. *Fear of crime of the respondents.*

Fearofcrime		Frequencies	Percent
	Yes	111	63.4
	No	64	36.6
	Total	175	100.0

Table 6 shows about 63% of total populations have fear of cyber crime.

Causes fear of cyber crime of the respondents

To define causes on fear of cyber crime had coded some value as like---in experience & unskilled, for weak operating

system, easily access, anonymity (vagueness).

Table 7. *Causes fear of cyber crime of the respondents.*

Causes fear of cyber crime	Frequencies	Percent
Unskilled & inexperienced	52	29.7
Weak operating system	38	21.7
easily access	17	9.7
anonymity(vagueness)	4	2.3
None	64	36.6
Total	175	100.0

Table 7 shows-Most student fear of crime for inexperienced & unskilled-about 52/29.7% pupils. For weak of operating system about 38/21.7% pupils & 17/9.7% noted the easily accessibility of total population. And also some about 2.3% fear for anonymity (vagueness)

Habit of use anti-virus & internet firewall & victimization situation of respondents

A concept "digital capable guardians" can be used in this case. In terms of the digital-capable guardianship, the three most common digital-capable guardians available to online users: antivirus programs, antispyware programs, and firewall programs. Each of digital guardians has its own distinctive function to protect computer system from computer criminals. First digital guardian, an antivirus program, mainly monitors whether computer viruses have gained an access through digital files, software, or hardware, and if the antivirus computer software finds a virus, the software attempts to delete or isolate it to prevent a threat to the computer system. The second digital guardian is a firewall program that is mainly designed to prevent computer criminals from accessing the computer system over the online network; however, unlike the antivirus software, firewalls do not detect or eliminate viruses [10]. The last digital guardian, antispyware program, is mainly designed to prevent spyware from being installed in the computer system [11].Once spyware is being installed, it intercepts users' valuable digital information such as passwords or credit card numbers as a user enters them into a Web form or other applications.

Here found the university student generally used two type of protective software as digital capable guardian-1.Antivirus software 2.Internet Firewall software. But they did not regularly use then fall in sever al problems. Again someone used regularly but then fall in victimization. By the following table we can easily imagine that.

Table 8. *Respondent faced cyber crime/victim.*

Bevictim	Frequencies	Percent
Yes	110	62.9
No	65	37.1
Total	175	100.0

Table 8 shows, 62.9% students are being victim of cyber crime.

Types of cyber crime faced pupils in public university (Types of victimization)

Targeting to make a digital Bangladesh by 2021, we have already stepped into the digital era. Lives will be much easier, quicker and meaningful if we use the digital facilities to perform our day-to-day activities. Once, people did not feel satisfaction if a printed news paper was not at their hands in the morning. Today, the same people feel nasty if the Internet is disconnected. It is very easy to think that we will be in a digital Bangladesh in few years. But very few people imagine that the digitalization without proper security measures will make our lives hell over night. Here founds ever all types of victimization as like

1. Virus attack, 50.3%.
2. hacking 2.86%
3. cheat chatting/stalking, 3.43%
4. Threat & harassment 6.29%

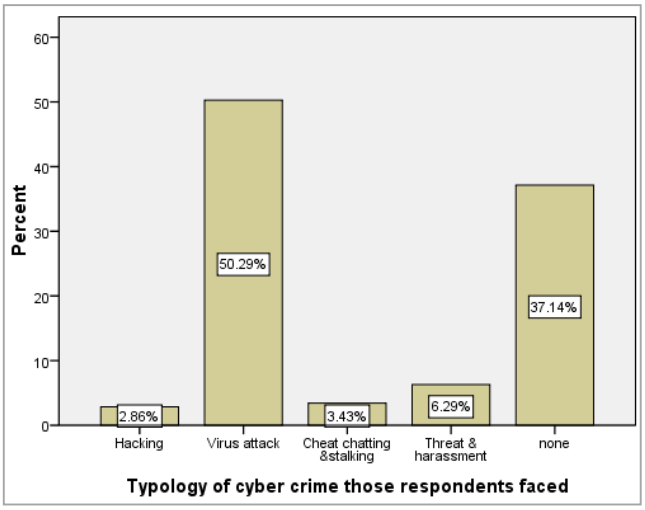

Figure 1. *Typology of cyber crime those respondents faced.*

Analysis some causal relationship on victimization & criminal activities of respondents

Passing duration of respondents with pc per day & Frequency of falling cybercrime:

There is a relationship among the passing duration & victimization & criminogenic traits of user because when they passed most time with it one's may be expert on it & gathered a lot of intellectuality to do cc but it is associated to be a victim. The field of cyber crime is open; there is no physical existence to secure: it is just secured by some programs when a person passing enough time then he/she will be capable to ensure the use of the programs). Generally a student of CSE & IT used pc almost all the time. Here took those periods whose are out of academic hours.

Here In the table we can see that, the frequency of cyber victimization is more which person passing more time with pc per day.

a Whose person those passed 9+ hours per day 3-6 times 3.4% & 1.1% 6-9 times, 1.1% faced 1-2 times.
b Whose person those passed 6-9 hours per day 3-6 times 8.6% & 1.7% 6-12 times 2.3% faced1-2 times.
c Whose person those passed 3-6 hours per day 3-6 times 5.7% & 1.1% 6-12 times12.0% faced1-2 times.
d Whose person those passed 1-2 hours per day 3-6 times 4.6 % & 0.6% 6-12times 20.0% faced 1-2 times.

Table 9. *Passing duration of respondents with pc per day & Frequency of falling cyber crime.*

			Frequency of falling cyber crime				Total
			1-2	3-6	6-12	None	
Passing duration of respondents with pc per day	1-3hour	Count	35	8	1	19	63
		% of Total	20.0%	4.6%	.6%	10.9%	36.0%
	3-6hour	Count	21	10	2	2	35
		% of Total	12.0%	5.7%	1.1%	1.1%	20.0%
	6-9hour	Count	4	15	3	2	24
		% of Total	2.3%	8.6%	1.7%	1.1%	13.7%
	9+hour	Count	2	6	2	0	10
		% of Total	1.1%	3.4%	1.1%	.0%	5.7%
	None	Count	1	0	0	42	43
		% of Total	.6%	.0%	.0%	24.0%	24.6%
Total		Count	63	39	8	65	175
		% of Total	36.0%	22.3%	4.6%	37.1%	100.0%

Table 10. *Most attractive site of respondents & Respondents face cyber crime.*

			Respondentsfacecybercrime		Total
			Yes	No	
Most attractive site of respondents	study materials	Count	22	12	34
		% of Total	12.6%	6.9%	19.4%
	Entertainment	Count	3	3	6
		% of Total	1.7%	1.7%	3.4%
	sports & games	Count	8	3	11
		% of Total	4.6%	1.7%	6.3%
	social site as facebook, yahoo, twitter etc	Count	48	12	60
		% of Total	27.4%	6.9%	34.3%
	sex related	Count	28	1	29
		% of Total	16.0%	.6%	16.6%
	None	Count	1	34	35
		% of Total	.6%	19.4%	20.0%
Total		Count	110	65	175
		% of Total	62.9%	37.1%	100.0%

Table 11. *Sex of the respondents & Typology of cyber crime those respondents faced.*

			Typology of cyber crime those respondents faced					Total
			Hacking	Virus attack	Cheat chatting & stalking	Threat & harassment	None	
Sex of the respondents	Male	Count	5	70	3	9	41	128
		% of Total	2.9%	40.0%	1.7%	5.1%	23.4%	73.1%
	Female	Count	0	18	3	2	24	47
		% of Total	.0%	10.3%	1.7%	1.1%	13.7%	26.9%
Total		Count	5	88	6	11	65	175
		% of Total	2.9%	50.3%	3.4%	6.3%	37.1%	100.0%

Most attractive site of respondents & Respondents face cyber crime

Here, most attractive site is an independent variable on which the victimization rate is depended. Several people like several things, internet also provide several information & services. People can survive their favorite site. Generally these private sites provide various offer & gifts in several times. Those people feel greediness they fall in victimization others, some people feel reserve & shyness in physical existence but in internet they can play role from hide id those type of people also faced several types of cc.

Table 10 shows that those people attracted with social site as facebook, yahoo, twitter etc those being victim most 27.4% because by those site they involve in chatting, feel greediness by several types of offer & being victim of fraud friendship as a result hacking, harassment stalking and so type victimization are faced. Again those peoples attracted by sex related site the tendency of being victim is more (about 16.0%) then others pupils.

From table 11 found that, male pupils are more attacked in various type of crime than female. About 40% male attract in virus but only 10.3% female are attacked in virus. Besides hacking rate & harassment victimization rate is also more than female. Then we can say that victimization don't depend on socio-demographic characteristics gender.

5. Conclusion

Cyber crime is still allowing priority to Bangladesh Police. As a whole Bangladesh is not aware of her cyber security. Though computer is becoming a common household item and the number of Internet users has already crossed six

millions, very few computer related offences are reported to the police. As our police have not been furnished with modern techniques and technology to investigate even traditional crimes, we cannot expect them to acquire the necessary skills to investigate the most complicated hi-tech computer related crimes. Victimization is a vast area of criminal occurrences that provide so much information about the criminal act; it was a heard work to define it in a small portion of study beside cyber victimization is a new form in Bangladesh. Generally when an online user accesses the Internet, personal information in his or her computer naturally carries valuable information into cyber space that attracts computer criminals. In addition, if computer criminals have sufficiently capable computer systems, the inertia of the crime target becomes almost weightless in cyber space. The nature of visibility and accessibility within the cyber-environment also allows the motivated cyber-offenders to detect crime targets and commit offenses from any where in the world. Internet on a regular basis based on the youthfulness of this new arena of communication and information, preventative programs, legislation, and technology to protect these youth from unwanted harassment and victimization while using the Internet are still in their infancy. In public university most of the victimization is occurred for various viruses although they used various types of anti-viruses programs but they cannot avoid it because an antivirus software play its role according to some programs that are fixed then an antivirus cannot catch all types of function those it's not been regarded & need to update. But many of our users are careless about it. Now cyber crime is a newly developed crime but the pattern & nature of cyber crime is increases day by day which causes so many types of crimes as like property crime, (credit card fraud. bank decoity etc), physical crime as like familiarity via cheat chatting causes even rape. So via cyber crime ever all types of crimes are raised then it is crying need to give the concentration on it. Arises various types of research projects to analysis measurement the types of cyber crime, criminal profile, patterns of victim & victimization process, effectiveness of law & operating systems of internet. The tools that have been developed and utilized as a protection device have been formed under the premonition that reducing the opportunity of online predators to victimize youth will in turn deter them from committing the crime.

References

[1] Power, R., 2001, 2001 CSI/FBI Computer Crime and Security Survey, Computer Security Issues and Trends, 7(1): 1-18.

[2] Gordon, L. A. et al., 2003, A Framework for Using Insurance for Cyber-Risk Management, Communications of the ACM, 46(3): 81-85.

[3] Jaishankar K., (2008).Space Transition Theory of Cyber Crimes.

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

[5] Hoffer, J.A., and D.W. Straub, 1989, The 9 to 5 Underground: Are You Policing Computer Crimes? Sloan Management Review (Summer1989): 35-43.

[6] Furnell, S. (2002). Cyber crime: Vandalizing the information society. Boston, MA: Addison-Wesley.

[7] Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44, 588-608.

[8] Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. European Society of Criminology, 2, 407-427.

[9] Robert Bohm, Keith Haley (2007), Introduction to Criminal Justice, McGraw-Hill press.

[10] Casey, E. (2000). Digital evidence and computer crime. London: Academic Press.

[11] Ramasastry, A. (2004). Cable News Network (CNN). com. Can Utah's new antispyware law work? Retrieved January16, 2016, from http://www.cnn.com/2004/LAW/06/03/ramasastry.spyware/index.html.