EUROPEAN ACADEMIC RESEARCH
Vol. II, Issue 8/ November 2014

Impact Factor: 3.1 (UIF)
DRJI Value: 5.9 (B+)

ISSN 2286-4822
www.euacademic.org

# Nature of the Cyber Crime Activities among the Secondary Student in Dhaka City of Bangladesh: A Baseline Study

Md. RAMJAN ALI
Student, Master of Education (M. Ed)
Institute of Education and Research, University of Dhaka
Dhaka, Bangladesh
REZVI SHAHARIAR
Lecturer
Institute of Information Technology, Dhaka University
Dhaka, Bangladesh

**Abstract:**

*Cyber crime is a concerning issue and threat for the information and communication technology (ICT) sector of Bangladesh. Significant numbers of Dhaka city dwellers mostly secondary level (13 to 19 years old) students are doing this unlawful crime consciously or unconsciously. Here, computer is used either as a tool or target or both. There is apparently no distinction between cyber and conventional crime. The differentiation lies in the involvement of the medium in cases of cyber crime. But the identification of crime and implementation of law both are new in our society. It indicates the frequent incidence of cyber crime among the secondary school students of Dhaka city. Hacking, credit card fraud, software piracy, cyber identity theft, cloning of website/phishing, pornography, cyber defamation, virus dissemination and cyber stalking are the common cyber crime in Dhaka City.*

**Key words:** Cyber crime, Secondary Student, Dhaka City, Information and Communication Technology (ICT), Information Society.

## 1. Introduction

Rights to information have become more and more important to everyone as information protects and develops human life every day. Understanding the essential need of security, almost all developed countries already have taken necessary steps to address the problem. On the other hand developing countries are far away from being able to guarantee this right. Bangladesh Government has already shown its commitment to Information and Communication Technology (ICT) through sharing the common vision of developing an Information Society, harnessing potential of ICT to promote development goals of the Millennium Declaration. Those include eradication of extreme poverty and hunger, achievement of universal primary education and development of global partnerships for the attainment of more peaceful, just and prosperous world. Along with other countries, Bangladesh Government has recognized the central role of science in the development of Information Society, the indispensable role of education, knowledge, information and communication in human progress, endeavor and welfare. Government has expressed its determination to empower the poor. Particularly those who are living in remote, rural and marginalized urban areas, to access information and to use ICTs as a tool to support their efforts to lift themselves out of poverty. So that present government declared vision 21: digital Bangladesh.

A safe and secure online environment enhances trust and confidence and contributes to a stable and productive community. Besides the increasing use and dependence on technology is one of the major influences on the domestic and international law enforcement operating environment. ICT impacts on law enforcement because of the way in which it can facilitate both lawful and unlawful activities. Crimes such as fraud, scams, and harassment can be facilitated by using technology which brings unique challenges to old crimes.

Activities which fall under this category are often referred to as high tech crime, computer crimes or cybercrimes. Under this study the nature of cybercrime activities among the secondary student of Dhaka city, Bangladesh try to be revealed.

## 2. Literature Review

The term 'cyber crime' is a misnomer. The concept of cyber crime is not radically different from the concept of conventional crime. Cyber crimes are divided into 3 categories: crimes where a computer is the target of the crime, crimes where a computer is a tool of the crime, and crimes where a computer is incidental to the commission of the crime (Brenner, 2009). Existing legal system and framework has shown inadequacy of law while dealing with Information Technology itself as well as while dealing with the changes induced by the Information Technology in the way of our living. The courts throughout the world have been dealing with these problems. Presently, the law (Statutory or otherwise) providing answers to these problems or dealing with the Information Technology is termed as 'Computer Laws' or 'Information Technology Laws' or 'Cyber laws' (WSIS 2005). Keeping the aims and objectives of the government in view, The Bangladesh Ministry of Science, Information and Communication Technology (MOSICT) has formulated some policies on protection of its growing cyber world from the unsolicited consequences.

The National ICT Policy, Cyber Law, Electronic Transaction Act are already adopted by the highest authority. Appropriate education on Computer Alert and Emergency Responses are underway by the different agencies including government, civil society/NGOs and private sector (Salim, 2005).

Paullet et al. (2012) said that sharing information on social network sites could potentially expose users to becoming victims of a cyber-related crime. Research has found that

students are worried about criminal activity such as identity theft, unauthorized access to online banking accounts, cyber stalking, cyber bullying, and child predators. Kamal, (2012) describes the nature of cyber crime which is committed in Bangladesh. As the use of internet in Bangladesh is not as wide as other developed countries, crime, however, related to internet is in emerging stage herein this country. It is revealed from the study that, though cyber crime is not in serious condition in research area, the respondents are victimized sometime by hacker, pornography sites and computer virus through internet. It is continuously growing attention of the majority people of the study area. Gandhi (2012) in his article considers

Cyber crime is an emerging serious threat. Worldwide governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are taking shape.

Author emphasized on the taking initiative to establish special cyber cells across the country and has started educating the personnel. This article is an attempt to provide a glimpse on cyber crime in India. This article is based on various reports from news media and news portal. From the above literature review it is clear that most of the study focuses on the nature and causes of cyber crime in their own way and country perspectives. But no study focused on any particular group of people. In this backdrop, the present study focuses mainly on the teenagers, how they engage cyber crime and the reasons behind this. Moreover, in Bangladesh a very limited number of studies have been conducted in this regard.

## 3. Theoretical Perspective

Sociological theories are form an integral part of sociological research as it is a general principle that explains or predict facts, observation or events. The theory of differential

association was adopted for this study. This theory was propounded by Edwin Sutherland an American Sociologist. Differential association theory proposed that through interaction with others, individuals learn the values, attitudes, techniques and motives for criminal behavior. According to this theory, the environment plays a major role in deciding which norms people learn to violate (Sutherland, 1939).

The principle of differential association asserts that a person becomes delinquents because of an "excess" of definitions favorable to violation of law over definitions unfavorable to violation of law. What this means is that an individual will become a criminal because they are exposed to more favorable criminal behavior. That is when one is exposed to more criminal influences rather than more favorable legal influences. In other word, criminal behavior emerges when one is exposed to more social message favoring misconduct than pro – social messages. This can be seen in environments with poor socio-economic conditions which may encourage negative views towards the law and authority.

According to Sutherland (1939), criminal behavior is learned. Criminal behavior is learned in interaction with other persons in a process of communication. This would mean an individual is influenced to participate in criminal behavior through watching and interacting with other individuals who are engaging in the criminal behavior. The principal part of the learning of criminal behavior occurs within intimate personal groups.

When criminal behavior is learned, the learning includes techniques of committing the crime, which are sometimes very complicated, sometimes simple and they learn the specific direction of motives, drives, rationalizations and attitudes for committing a crime. This means that an individual will be influenced into believing that the behavior which they may have previously believed was wrong, into believing that it is right through rationalization of their action.

Furthermore, an individual will be pushed into deviant behavior depending on their view of the legal code as being favorable or unfavorable. A person becomes delinquent because of an excess of definitions favorable to violation of law over definitions unfavorable to violation of the law. Therefore, an individual will break a law if they see more reasons to break it than to stay in compliance with it. Differential Associations may also vary in frequency, duration, priority and intensity. The process of learning criminal behavior by association with criminal and anti-criminal patterns involves all of the mechanisms that are involved in any other learning. This means that individuals learn criminal actions and legal through the same way. This theory states that while criminal behavior is an expression of general needs and values, it is not necessarily the fulfillment of these needs and values which causes deviant behavior since non-criminal behavior is an expression of these same needs and values.

The theory of Differential Association can be applied to cyber crimes. The main premise behind this theory is that criminal behavior is learned through social interactions with others. The profile of cyber criminals is one who is very smart, highly knowledgeable and who are computer savvy. Their social interactions may come through electronic communications with other individuals who share similar technological interests. If they do not currently have any desire to commit malicious acts through electronic means, such as an act in violation of the computer fraud and abuse act, then they may become influenced through another individual with whom they share electronic communications. This theory which was developed to help explain white collar crime fits in well with those who violate or commit cyber crime. There are a wide spectrum of the different kind of offenders and motivations.

## 4. Conceptual *Framework:*


## 5. Statement of Problem

Bangladesh is a country of young age structure. Almost 52% of its population is below 25 years. At least 40% of its population consists of teenage and those are mainly studying in the secondary level of formal education in Bangladesh. With the improvement of technology, approximation is that majority of these teenagers are the prime users of the ICT. Again from literature various studies revealed that in developing countries majority of cyber criminals are children and adolescents between the age group of 6 to 18 years. So considering the fact it is reasonable that in context of Bangladesh the scenario would be the same. As the young age people are more expose to cyber activity than their guardians so the cultural gap is there and exposing the young age people in to a new dimension of global world. Under such circumstances present study is going to inquiry the present scenario among the secondary level student about the extent and nature of cyber accessibility and its coherence cyber crime proximity.

## 6. Research Objectives

The overall purpose of the study is to identify the extent of cybercrime in Dhaka city of Bangladesh with regard to technological enhancement among the young age people.

- To explore the computer and internet using situation among the secondary student of Dhaka city, Bangladesh.
- To point out the various types of cyber crimes among the secondary student of Dhaka city.
- To discover the profile of cyber criminals among the secondary student of Dhaka city.
- To explore the profile of cyber crime victims among the secondary student of Dhaka city.
- To find out the causes of cyber crime in Dhaka city.

## 7. Significance of the study

Communication has become one of the most crucial integration ways in world. It has change the dimension of people society and connectivity. So interaction of lots also raises issues of order and violation of norms. Even mass gathering and public movements are organized through information communication way. Arab springs, *gonojagoron* movements are the evidence of such activities. Again sabotaging of such movements through the internet is also well publicized in our country. So, present study will definitely add vital information to understand such communication approach in more details to counter the odds in future incidents.

## 8. Methodology

This study is quantitative and exploratory by nature and it based on primary data collected from the questionnaire survey. All secondary level students of Dhaka city are the population of this study. To fulfillment of purposes of this study non-probability sampling techniques are used to select the respondents. The non-probability sampling methods are the purposive and snow ball sampling. Samples are selected from the age group 13-19 years old whose are now studying in the secondary level of Education in Bangladesh. Among of them

75% respondents are male and 25% are female. At the same time 70% respondents are Muslim and 30% respondents are Hindu religion. Among of the total respondents 75 % are unmarried, 25% are married and only 1 respondent is divorced. The study is confined in all Thanas of Dhaka District, Bangladesh. For analyzing the data obtained from questionnaire a descriptive approach is used. Different themes related to 'cyber crime' are identified and data are analyzed under each theme. Simple percentages of respondents against the supplied evidence are computed for questionnaire.

## 9. Findings and Discussion

### 9.1Computer and Internet using situation

This section examines the computer and internet using situation among the secondary student of Dhaka city, Bangladesh. It identified the situation of computer and other electronic devices use, purpose or reasons to use these devices, internet accessibility and the cost of internet of the respondents.

It is explored that around 95% respondents of this study are used computer or other electronic devices to their daily activities. On the other hand, only 5% say that they are not used computer or other electronic devices. They use these devices for their different purposes. These are mentioned in the following figure 1.

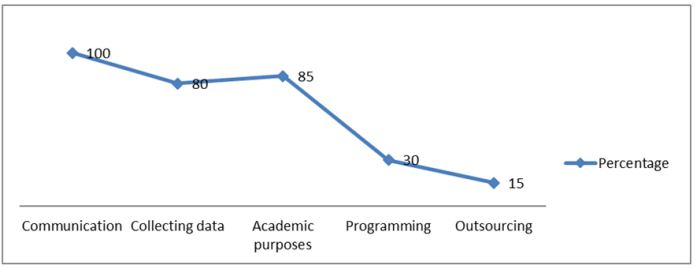


**Figure 1: Reasons of using these devices**

Figure 1 shows that all the respondents (100%) use these devices for communication purpose. Some other respondents use these devices for various purposes like collecting data (80%), academic purposes 85%, outsourcing 15% and programming 30%.

It is a good sign that only 6 respondents among the 120 respondents do not have internet access. That means 95% respondents (6 out of 120) use internet while they use various electronic devices.

**Table 1: Monthly expenditure of money for internet**

| | *Responses* | |
|---|---|---|
| *Monthly expenditure for internet use* | *Frequency* | *Percentage* |
| Less than tk.300 | 66 | 55 |
| Tk.301-500 | 24 | 20 |
| Tk.501-700 | 12 | 10 |
| Tk.701 and above | 18 | 15 |
| Total: | 120 | 100 |

According to the Table 1, 55% respondents expend tk. 300 monthly, 20 respondents say that they expend tk. 301- 500. On the other hand, less per cent of respondent (15%) use tk. 701 0r above.

### 9.2 Knowledge about cyber crime

It is explored that almost all respondents (90%) are familiar with the term cyber crime. They know what types of activities are considered as the cyber crime and how these are happening. On the other hand only 10% are not familiar with cybercrime.

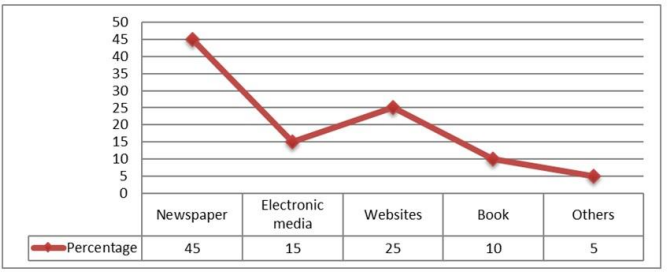


**Figure 2: Where respondents know about cyber crime**

Figure 2 reveals that 45% respondents get information about cybercrime from newspaper. Among of the respondents 25% have got information from various websites, 15% get information from various electronic media.

### 9.3 Profile of cyber criminals

It is explored that 70% respondents consider that youth are mainly involving in cyber crime. On the other hand 25% respondents are also said about Adult and another 5% are also said about Aged people. That means 70% youths are involved in cyber crime somehow. On the other hand 25% adult people and only 5% aged people involved in cyber crime according to the respondents. Respondents are also said that most of the cyber criminal are in the age group of 13 to 18. Simultaneously, 25 per cent are also said about 19 and above aged people. On the other hand, only 10 per cent respondents say about the 7-12 age groups.

### 9.4 Types of cyber crime

Respondents are mentioned a number of cyber crime. Hacking, credit card fraud, software piracy, cyber identity theft, cloning of website/phishing, pornography, cyber defamation, malicious program/ virus dissemination and cyber stalking are the common crime in Bangladesh. The following table 2 is presenting these crimes.

**Table 2: Activities considered as cyber crime**

| | *Responses* | |
|---|---|---|
| *Activities considered as cybercrime* | *Frequency* | *Percentage* |
| Hacking | 90 | 75 |
| Credit card fraud | 0 | 0 |
| Software piracy | 114 | 95 |
| Cyber identity theft | 18 | 15 |
| Cloning of website/Phishing | 6 | 5 |
| Pornography | 108 | 90 |
| Cyber defamation | 0 | 0 |
| Malicious program/ Virus dissemination | 36 | 30 |
| Cyber stalking | 18 | 15 |
| Total: | 390 | 325 |

According to the above table 2 it demos that pornography and hacking is common activities that are considered as the cyber crime (90% and 75% respectively). 15% think of identity theft, 30% call on behalf of malicious program or virus dissemination. It is also explored that 80% respondents downloaded copyrighted files from internet. Conversely, only 20% do not admit this. At the same time 95% respondents have installed pirated software and 5% do not installed pirated software. They are also used pirated software that are downloaded (55%) from internet and 45% brought from an IT shop.

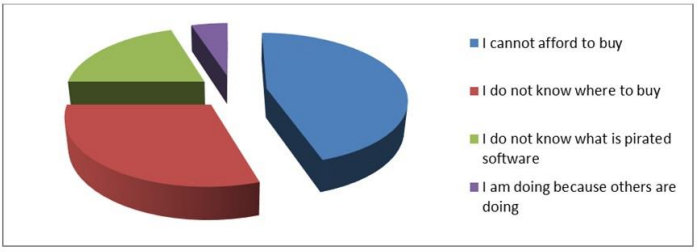


**Figure 3: Reasons to install the cracked software**

The above figure 3 demonstrates the reasons to install the cracked software. Here, 45% respondents utter that they do not

have the afford to buy so that they installed cracked software. Simultaneously, 30% respondents do not know where to buy and 20% respondents do not know what pirated software is. On the other hand, only 5% respondents say that they are using because others are using.

Some people are also copied text from internet without crediting (90%) and 10% do this. They do this crime for assignment (80%) purpose and 20% for publication purpose. Some are also said that the photograph without getting any permission from the owner of the photo.

### 9.5 Profile of the cyber crime victims

Fifty per cent of the total respondents tell that they are the victim of hacking and only 50% are not victims for a single time. That means hacking rate of our country is now in the concerning stage.

**Table 3: Sites of hacked**

| | *Responses* | |
|---|---|---|
| *Where is the hacking occurred* | *Frequency* | *Percentage* |
| Email | 24 | 40% |
| Blog | 0 | 0% |
| Social network | 36 | 60% |
| Others | 0 | 0% |
| Total: | 60 | 100% |

The table 3 presents the side of hacked. Here, 60% respondents say that among the victims of hacking are hacked in social network sites and 40% were by email account. Because these two sides are the most used sides in Dhaka city of Bangladesh.

**Table 4: Victims of cyber crime**

| *Victims of cybercrime* | *Responses* | |
|---|---|---|
| | *Frequency* | *Percentage* |
| Male | 30 | 25 |
| Female | 60 | 50 |
| Business organization | 18 | 15 |

| | | |
|---|---|---|
| Bank and govt. office | 12 | 10 |
| Total | 120 | 100 |

This table 4 demonstrates that female is the main victims (50%) of cyber crime where as male (25%) and business organization and bank are 15% and 10% respectively.

### 9.6 Causes of cyber crime

It is explored that various reasons are working behind this crime. Among of them unemployment, poverty, peer group influence, defective socialization, weak laws, corruption and easy accessibility to internet are most vital reasons of cyber crime in Bangladesh.

**Table 5: causes of cyber crime**

| | *Responses* | |
|---|---|---|
| *Causes of cybercrime* | *Frequency* | *Percentage* |
| Unemployment | 90 | 75 |
| Poverty | 90 | 75 |
| Peer group influence | 96 | 80 |
| Defective socialization | 78 | 65 |
| Weak laws | 114 | 95 |
| Corruption | 90 | 75 |
| Easy accessibility to internet | 90 | 75 |
| Total: | 648 | 540 |

This table 5 draws the attention of the causes of cyber crime. Among the respondents 95% think that weak laws are the main reasons of cyber crime.

## 10. Conclusion

Cybercrime is a double aged sword. It is very common phenomenon at present time. The current study try to reveals the nature and proximity of cyber crime among secondary students of Dhaka City. It is seen that the secondary level student (teenagers) are more or less commit cyber crime

somehow consciously and sometimes unconsciously. They have limited knowledge about the ICT Act. Moreover, lack of proper monitoring and application of Act, teenagers involved in cyber crime. So, general people along with government should come forward to stop this crime.

## 11. Recommendations

Education is the most vital weapon to in light people, so that government can include a content or course in the secondary and higher secondary curriculum of Bangladesh formal education system. So that government and non-government organization can organize seminars and workshops frequently with emphasis on cyber safety so that the individuals will learn to keep their personal information safe and youth will flee cybercrime.

New laws and acts on cyber crime are also needed to employ in practice. For that law enforcing agencies like police, RAB etc can play a vital role to control or prevent cyber crime in Bangladesh. So that government can make a provision for intensive training of law enforcement agencies on ICT so that they can track down the cyber criminals no matter how intelligent and cunning they may be.

## BIBLIOGRAPHY

Agba, P.C. (2002), *International Communication Principles, Concepts and Issues*. In Okunna, C.S. (ed) Techniques of Mass Communication: A Multi-dimentional Approach. Enugu: New Generation Books.

Akogwu, S. (2012),*An Assessment of the Level of Awareness on Cyber Crime among Internet Users in Ahmadu Bello University*, Zaria (Unpublished B.Sc project). Department of Sociology, Ahmadu Bello University,

Ayantokun, O. (2006), *Fighting Cyber crime in Nigeria: Information system*.www.tribune.com

Brenner, S. (2009). *Cybercrime: Challenges foe law enforcement*. Dayton: Law and Technology University of Dayton. Retrieved September 15, 2014 form: https://www.defcon.org/images/defcon-11/dc-11presentations/dc-11 -Brenner-Susan/dc-11-brenner.pdf

Ehimen, O.R. & Bola, A, (2010), *Cybercrime in Nigeria.* Business Intelligence Journal, 3(1) January 2010

Gandhi, V.K. (2012). *An Overview Study on Cyber crimes in Internet.* Journal of Information Engineering and Applications, 2(1). New York: The International Institute for Science, Technology and Education (IISTE).

Kamal, M. M et al. (2012) . *Nature of Cyber Crime and Its Impacts on Young People: A Case from Bangladesh.* Asian Social Science.8(15). Toronto: Canadian Center of Science and Education

Kumar, K. (2003), Cyber Laws, International Property and e-commerce Security. Dominant Publishers and Distributors, New Delhi.

Mc Connell (2000), *Cyber crime and Punishment*. Archaic Law Threaten.

Olaide & Adewole (2004*), Cyber Crime Embarrassing for Victims.* Retrieved May 2014 from http//www.heraldsun.com.au

Olugbodi, K. (2010), *Fighting Cyber Crime in Nigeria.* Retrieved April 10, 2014 from http//www.guide2nigeria,com/news_articles_About_ Nigeria

Oyewole & Obeta (2002), *An Introduction to Cyber Crime.* Retrieved September 2013 from http//www.crime-research.org/articules/cyber-crime.

Paullet et al. (2013). *Cyber forensics and information security: A new and innovative bachelor's degree program*. Issues in Information Systems, 14(1). Retrieved September 15,

2014 from: http://iacis.org/iis/2013/204_iis_2013_244-250.pdf

Ribadu, E. (2007),*Cyber Crime and Commercial Fraud; A Nigerian Perspective*. A paper presented at the Modern Law for Global Commerce, Vienna 9th – 12th July.

Salim, R.(2005). *Cyber Security Bangladesh Perspectives*. Paper prepared for ITU WSIS Thematic Meeting on Cyber Security ITU Headquarters, Geneva, Switzerland June 28 - July 1, 2005. Retrieved September 16, 2014 from: http://www.itu.int/osg/spu/cybersecurity/contributions/Bangladesh_Salim_paper.pdf

Shinder, D.L.(2002), Scene of the Cyber crime: Computer Forensics Handbook. Syngress Publishing Inc. 88 Hingham Street, USA.

Sutherland, E.(1939), Principles of Criminology. Fourth edition.

WSIS (The World Summit on the Information Society) 2005

Vladimir, G.(2005), International Cooperation in Fighting Cyber Crime. www.crimeresearch.org

Zaria. A. J. (2009), Fighting Cyber Crime in Nigeria. Retrieved October 24, 2014 from: http://www.jidaw.com/itsolutions/security3.html.