Asian Social Science; Vol. 8, No. 15; 2012
ISSN 1911-2017 E-ISSN 1911-2025
Published by Canadian Center of Science and Education

Nature of Cyber Crime and Its Impacts on Young People: A Case from Bangladesh

Mohammad Mostufa Kamal[1], Iqbal Ahmed Chowdhury[1], Nadia Haque[1], Mydul Islam Chowdhury[1] & Mohammad Nazrul Islam[1]

[1] Department of Sociology, Shahjalal University of Science and Technology, Sylhet, Bangladesh

Correspondence: Iqbal Ahmed Chowdhury, Department of Sociology, Shahjalal University of Science and Technology, Sylhet-3114, Bangladesh. E-mail: Iqbal_chy@yahoo.com

Received: August 29, 2012 Accepted: September 27, 2012 Online Published: November 30, 2012

doi:10.5539/ass.v8n15p171 URL: http://dx.doi.org/10.5539/ass.v8n15p171

Abstract

Cyber crime is known to all over the world as a crime committed through internet. It is, nowadays, becoming a serious matter of concern all over the world. This paper 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. The study is exploratory in nature. Methodological triangulation (face to face interview and case study) has been applied to collect pertinent data from 30 purposively selected respondents. 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.

Keywords: crime, cyber crime, internet, computer hacking, pornography, identity loss, hacking, computer virus

1. Introduction

Internet is becoming popular day by day because of its some special features. A revolutionary change has come in communication and socio-economic transaction by internet. Being facilitated with the virtue of it, people can communicate very easily national as well as international level. Generally it is called on-line communication. It is the vast source of information. We can get any information from the Internet. Though it is the easiest way of communication, now it is the matter of concern that misuse of computer and internet put together some people to commit crime. According to Council of Europe "Any criminal offence committed against or with the help of a computer network is identified as cyber crime" (Council of Europe Convention on Cybercrime 2001:8). So computer is must for cybercrime. Generally Among the numerous crimes in today's society; cybercrime has become very common as well as very dangerous. The emergence of new technology has increased the number of perpetrators that take advantage of these resources to use them illegally for their own gain (Gjata 2007:5).

The most dangerous aspect of cybercrime is that the victims fail to acknowledge the cause of their unfortunate fate. Not only should victims report any sort of suspicion and/or crime, but the victim needs to identify the suspected machine so police can confiscate it in order to have evidence gathered form the machine's hard drive.

Without having the computer form which the perpetrator committed his crime(s) then it is very hard to convict and persecute these perpetrators. Victims of cybercrime need to become aware of such crimes and they need to become more educated in how to protect and prevent not only themselves but others as well from such malicious acts.

With today's advanced technology the urgent need of information security, ethical education and awareness programs cannot be emphasize enough in order to achieve the maximum protection from the hackers and also to protect Cyber world from our own abusive use (Gjata, cybercrime 2007: 7)

Numerous government agencies around the world have taken necessary precautions to detect and persecute perpetrators of cybercrime. Although, because of the vast amount of new technology being produces regularly government agencies have to stay alert and informed in order to control cybercrime. Cybercrime can be victimless, but it can also harm unfortunate individuals.

1.1 A note on Cybercrime

Cybercrime is a worldwide problem now; no country is immune (El-Guindy 2008: 16). The first cybercrimes occurred in India, Japan and china in 1820(Techno focus cybercrime-A looming threat 2008). After that it was increasing evolutionary and at mid of 20th century it became a problem of concern. Around the world and in Middle East and third world countries the growth of Internet connectivity in recent years is significant and simultaneously similar increase in cybercriminal activities (El-Guindy 2008:16). We see in 2001 approximately 28.5 million people in the UK use the Internet (Fafinski 2008:1). Internet use in the Middle East had reached 2.5% of the total worldwide use by December 2007(El-Guindy 2008:3). 50% adult use Internet in Australia (Australian federal police: 4). In Bangladesh Internet was first introduced in 1996(Hossain 2004:6). Foskett said Internet users are growing rapidly in Bangladesh especially in the metropolitan areas. In 2000, the number of Internet users was 100,000 and it shot up to 450,000 in 2007(www.crime-research.org/news/07.11.2007/2995/). In another report says about 2 million people use internet in Bangladesh (Hossain 2004:6) In Canada by the year 2000 the 45,950 computer crimes reported by the NIBRS2 and noted that most common type of computer crime was larceny/theft (Kowalski 2002:12). By the years cybercrimes develop besides technical development and by time it created new dimension of crime such as from telecommunication crime to electronic money laundering (Graycar 2000). Because of cybercrime people lost their money, identity and many more.

In the UK there were 92000 cases of on-line identity fraud during 2006 because of that average value of loss from 183.2 to 212.6 million pounds by card-not-present (CNP) fraud. 218.817 incidents of physical harassment were recorded. In 2006 850000 cases of unwanted online sexual approaches occurred (Fafinski 2008:8-14). 38% Drug Importation cases, 34% Defraud the commonwealth cases, 25% Child Sex related cases, 3% Counterfeit currency/documents cases, 45% E-Crime, 11% Interpol, 2% Counter terrorism, 42% Others (Fraud, Credit Card, Money Laundering) occurred in Australia during 2005 and 2006 (Australian federal police: 4-5). The systems of NASA, US Army, Navy and Department of Defence were hacked right after the 9/11 attacks (www.crime-research.org/news/13.01.2009/3692/). Spam is now a great problem in cyber world everyday thousands of Spam spreading through e-mail and other way. Nearly 200 billion Spam messages are now sent each day, double the volume in 2007 — and that targeted attacks are also rising sharply and 90 percent of all e-mails sent worldwide are Spam, this means 800 million messages a day are attempts are spear phishing (www.crime-research.org/latest news/18.12.2008/3681/). One in four (23%) of UK internet users had been victim of phishing scams during the last 12 months, compared to just eight per cent the year before. Similarly, more than one in six (16%) had fallen victim to other types of online scam (www.theregister.co.uk/2009/02/10/safer_internet_day.htm).

One of the most important issues is child pornography. Because of the Internet pornography industries generate approximately 3 billion US dollars annually and there are roughly100000 websites offering illegal child pornography (Young 2008:287). In Tahlequah Michael Ray Wright had pictures of underaged girls during April 1 & Dec 18, 2008 (www.crime -research.org/latest news/14.01.2009/3693/). Australian Broadcasting Authority found 54% credit card number theft, 45% personal data misuse, 39% privacy issues and 21% incidents because of viruses (Barbara 2002: 4). On the top of the list of cybercrimes registered in 2006 there are 1.94 million cases of harassment, this figures includes e-mails with threatening or abusive statements and offensive allegations left on websites and about 850,000sex crimes including cyber stalking occurred in Britain (www.infoniac.com/hi-tech.htm).

Considering the contemporary and early history it is found, 1st world countries are most affected because they were reported but we have no chronological data about cybercrime in our country. The impact of cyber crime is not as alarming in Bangladesh because financial transactions have not yet been fully facilitated online, said Freddy Tan, chief security advisor of Microsoft Southeast Asia. He warned that, as soon as financial transactions are allowed, online computer crimes would increase at an unprecedented rate, unless the government acquires the tools and infrastructure to prevent, detect and prosecute them. 'Online financial scams are a major threat for banks, credit card holders and alike.' 'Internet services provided through the local area network are vulnerable to similar attacks and intrusions by hackers more often when security level was inadequate. According to a government study conducted by the Bangladesh computer council, only 0.3 % of the total population own computers and 0.7% have access to the Internet. The government statistics for cybercrime are not remarkable, but district judge have been empowered to try cases in reference to the panel code of criminal procedure. The limited number of cybercrime apprehended is confined to e-mail threat (Hammadi 2008: 2-4). An example is that E-mail threatening to such organization and renowned person in Bangladesh (Borhan Uddin 2006: 14).

Bangladesh government has launched the initiative of making digital Bangladesh. But the use of internet is limited in this country. People mainly use internet for their educational purpose. Bangladesh is a safe haven for

anyone committing a computer crime. From viruses (which infect computers to malfunction), Trojans (deceptive software or malware that appears to perform an action but instead performs another) and Spam to online threats, piracy, hacking (accounts), theft (of data or pin numbers) and pornography, all these facts of computer crime have advanced significantly beyond existing modes of detection So there is no doubt that how important matter that is for the contemporary situations in Bangladesh at the rising time of Internet technology.

2. Objectives

The broad and general objective of this research is to find out and describe the nature of cybercrime by which the young people, who use Internet, are affected and the impact of it.

This broad objective has been splinted into several specific objectives. These are,

1) To know the types of cybercrime by which the young people are effected;

2) To know the realization of victim about cyber crime; and

3) To know the effects of cybercrime upon the victims.

3. Methodology

The research has been conducted on Sylhet City Corporation in Bangladesh. Explorative research design has been used in this research to explore the real situation of cybercrime in this area and the consciousness of internet users (young) about this crime. The population of this research is not finite because internet users in cybercafés could not be counted. So, people who use internet (of age group 18 to 30) have been counted at several cybercafes in research area. Non-probability accidental sampling technique has been applied to select the sample because of the nonfinite population and the sample size is 30. Data have been collected through methodological triangulation method- Social survey (face to face interview with questionnaire) and case study to get in-depth information about the problem. After getting data, simple statistical tools like univariate analysis; mean, median and mode have been used to analyze data.

3.1 Crime and Cyber Crime

The crime committed in Cyber world is a common matter of present world. Basically Cybercrime is a complex crime and its range is so vast. There is no specific or all accepted definition of cybercrime because different agencies and researchers gave the definition according to their place and situation. It can say the cybercrimes are that crimes which have the involvement of computer and network (Fafinski 2008:2, Kowalski 2002:7, www. Definitions and general information [Cybercrime].htm).To given the definition of cybercrime some researchers told that the crime committed with internet and information technology (Sheridan 2004, Cybercrime - Wikipedia, the free encyclopedia.htm). It has some different name such as computer crime", "computer-related crime", "high-tech crime", "Internet crime"(Brenner and Goodman 2002:6, Kowalski 2002:7).

There are many types of cybercrime existing in present world. It is very difficult to find out all types of cybercrime because everyday the new dimension of cybercrime is inventing. We can cite few types of cybercrime, which occur generally in every place of the world. "Identity fraud" is a type (Blindell 2006:6, Fafinski 2008:4, ACPR 2006, parliamentary joint committee on the Australian crime commission 2004:43, Brenner and Goodman 2002: 7). It is defined as "The assumption of the identity of another person, living or dead, irrespective of the motivation underlying this courses of actions"(Fafinski 2008: 4). Identity fraud is used as a means to commit drug, firearms and e-crime offences (parliamentary joint committee on the Australian crime commission 2004:44). Identity fraud refers to the gaining of money, goods, services or other benefits through the use of a false identity (ACPR 2006:14). In the United States of America, the term 'Identity theft' is generally used to cover all types of identity crime, The United Kingdom government appears to use 'identity fraud' as a generic term, In Australia, definitions adopted within policing entail the use of 'identity crime' as a generic description to cover all types of identity crime (ACPR 2006: 5). Another type of cybercrime is "Financial Fraud" (Fafinski 2008: 3,Graycer 2000: 8). It is defined as the use of deception for direct or indirect Financial or material gain (Fafinski 2008: 4). It includes Internet banking, credit and debit card fraud, and money laundering (Graycer 2000:8, parliamentary joint committee on the Australian crime commission 2004:47). In the context of credit card, financial fraud defied as "unlawfully obtained credit card numbers to order goods or services online" (Kowalski 2002:15). "Offences against the person" is a common type of cybercrime (Fafinski 2008: 3). It includes the use of a computer to cause an individual some form of personal harm such as anxiety, distress or psychological harm, precisely we can say threatening e-mails and the posting of derogatory information online is the best example of that crime (Fafinski 2008: 5). Another type "Computer misuse" means unauthorized access to a computer system such as "basic hacking", "aggravated hacking" and unauthorized modification of computer material such as "viruses"(Fafinski 2008: 3). "Sexual offences" is most concerning types of cybercrime at

present because of the availability of pornography (Fafinski 2008: 3). We can also give a relevant name that is "Pornography And Other Offenses Against Morality" it includes child pornography and other offenses against minors, stalking, harassment, hate speech etc (Brenner and Goodman 2002:10). This category of cybercrime covers a range of conduct that has an objectively ascertainable sexual elements including pedophilic activity such as grooming a child for sexual activity. At present "Spam", "Phishing", "Botnets" are the matter of concern at Cyberworld because it causes lots of harm of computer system and data management (Jaishankar, Pang and Hyde 2007: 258). "Theft of Telecommunications Services" The "phone phreakers" do it by gaining access to an organisation's telephone switchboard (PBX) individuals or criminal organisations can obtain access to dial-in/dial-out circuits and then make their own calls or sell call time to third parties (Graycer 2000:1). Telecommunications Piracy means the temptation to reproduce copyrighted material for personal use, for sale at a lower price, or indeed, for free distribution, has proven irresistible to many (Graycer 2000:3).

3.2 Effects of Cybercrime

People in the whole world are affecting by cybercrime all time but most of the cases are unreported. In the UK there were 92,000 cases of online identity fraud during 2006. Around 40% of all identity frauds are facilitated online. The most stolen documents used by fraudsters were utility bills, passports and bank statements (Fafinski 2008: 8). 10% people in Australia suffered by on-line frauds (AFP 2006: 9). In 2000, of the 45,950 computer crimes reported by the NIBRS2, 5,744 were crimes where the computer was the tool and 40,211 were crimes where the computer was the object. The most common type of computer crime for both definitions was larceny/theft (Kowalski 2002: 12). Internet Crime Complaint Center (IC3) reported that 206,884 complaints were filed online for an estimated $239 million loss in 2007(www.crime-research.org/news/29.01.2009/3702)

In Britain it is estimated that there were 207,000 cases of online financial fraud during 2006,among them Card-not-present (CNP) fraud was 49% and the total value of loss of CNP fraud are from £183.2M to £212.6M (Fafinski 2008: 10). About 42% financial fraud (Fraud, Credit Card, Money Laundering) occurred in Australia during the year 2005 and 2006 (AFP 2007:7-9). In the Middle East over the past few years banks lost approximately one billion dollars to organized cybercrime on online transactions and most banks in the region are vulnerable to phishing attacks (El-Guindy 2008:16). UK banking association APACs warned that online banking fraud losses were £21.4m in the six months to June 2008(www.theregister.co.uk/2009/02/10/safer_internet_day/). FBI survey reported that the annual loss due to computer crime was estimated at $67 billion for U.S.A in 2005 (www.crime-research.org/news/29.01.2009/3702).

By the innovation of the Internet and the World Wide Web (WWW) has created a fictitious world filled with an unlimited amount of information, which dramatically changed the underground world of child pornography. By unexpectedly becoming the new medium for intent, motive, and ambition, the Internet has become a vital part of the child pornographer's criminal tradecraft (Seigfried, Lovely and Rogers 2008:286-287). Half (49%) of Canadians have come across websites that contain pornography. Of those that have come across pornographic websites, 83% came across it unexpectedly and 46% found it offensive. 13% of Internet users came across content that promotes hate or violence to a particular group. 8% of Canadians who used the Internet had received threatening or harassing e-mail (Kowalski 2002: 15). Australian Federal Police reported that about 35% Child Pornography, 8% Child Grooming (using the internet and mobile phones), 4% Family Violence/Sexual Assaults occurred in Australia during the year 2005 and 2006 (AFP 2007:7-9). In Britain during 2008 there were 500 new cases of online child abuse reported every month (www.theregister.co.uk/2009/02/ 10/safer_internet _day). In Tahlequah a criminal took some pictures of undressed girls illegally and posted the pictures to their family and showed them exposing themselves, after proving that this criminal was accused and sent her to jail and financial punishment (www.crime-research.org/news/14.01.2009/3696/). In Britain 1,944,000 cases of online harassment placed during 2006 (Fafinski 2008: 12).

Cisco Systems Inc. found an alarming increase in the amount of personalized spam, which online identity thieves create using stolen lists of e-mail addresses or other poached data about their victims. Spam is growing quickly nearly 200 billion spam messages are now sent each day, double the volume in 2007 and that targeted attacks are also rising sharply. About 800 million messages a day are attempts are spear phishing in SANFRANSISCO (www.crime-research.org/news/18.12.2008/6381/). One in four (23 per cent) of UK internet users surveyed reckon either they or their close friends and family had been a victim of phishing scams during the last 12 months (www.theregister.co.uk/2009/02/10/safer_internet_day/). In Bangladesh, Prime Minister Sheikh Hasina got a threat by e-mail from a cybercafe and World Bank, Dhaka office got a threat through e-mail (Borhanuddin 2006:14).

Virus is the new dimension of cybercrime. About 6,000,000 virus incidents took place in Britain during 2006(Fafinski 2008:13). A virus named "Love Bug" which destroyed files and stole passwords. The virus was ultimately estimated to have affected at least forty-five million users in more than twenty countries. NASA and CIA also affected through this virus (Brenner and Goodman 2002:2)."Hacking" is a specific concept of stolen data and information from any computer through network. In Bangladesh lots of incident occurred during last year such as stolen the transactions report of Dhaka Stock Exchange, Hacking the e-mail of BRAC Bangladesh, Inserted porno movies in the website of Bangladesh national parliament, Jamate Islami Bangladesh, the Daily Jugantor (Borhanuddin 2006:14).

Theft of telecommunication services occur everyday in the world .Computer hackers in the United States illegally obtained access to Scotland Yard's telephone network and made £620,000 worth of international calls and Scotland yards had to responsible to pay that bill(Grayacer 2000:1). A hacker broke the voice-mail system of HUB Computer Solutions in Winnipeg and made calls worth of $43,000 and the company had to pay that unwanted bill (www.crime-research.org/news/24.12.2008/3684).Thieves hacked the Internet phone systems of WA businesses and used the phone system to make more than 11,000 international telephone calls in 46 hours that worth $120,000 and the Company paid that amount (www.crime-research.org/news/20.01.2009/3694/)

4. Findings and Discussion

The data collected on the nature and impacts of cyber crime are analyzed below,

According to the respondents (see Table 1) (40%) are 23-26 years in age, more than a quarter (33.3%) of Internet users are 18-22 years in age and about a quarter(26.7%) users' are 27-30 years old. The people who are 23-26 in age use internet more (Case-1&4) because, at present, students get easy access into internet for their study purpose and they want to keep in touch of modern technology because of globalization (Table 3). They are being victimized of cyber crime easily. Table 2 shows that maximum (93%) of internet users are male and a little percent (6.7%) are female. The main reason of few female members is that they don't feel social security at cybercafes. Table 3 focuses on the level of education of the respondents. More than half (53.3%) users studying in graduation level, less than a quarter (20%) are masters' level and about a quarter (23%) are HSC level. A very percent like 3.3% are SSC level. So, majority of the respondents are in graduate level. It, therefore, can be said that educated users are using Internet in Sylhet City. From table 4, it is, seen maximum Internet users are students (63.3%). A small number of service holder and private serviceman use Internet (16.7% each). Rest is unemployed (3.3%). More than half respondents are students. So, it is clear that in Sylhet city students use Internet more than other people. From table 5 we get majority (40%) users have been using Internet for 4-6 years (see Case 3, 4). The percent of new users, who are using Internet during 1-3 years, is 33.3% and the percent of experienced users are very little that is 26.7%. In aspect of Bangladesh, people use Internet from a teenage, not from childhood. Because, internet facility has not yet gone to home smoothly. From table 6 we can see that, a great number of users use Internet regularly (Case-1, 2, 3) for different need of their life and it has, by and large, become a necessary part of their life. More than three out of five (73.3%) users use Internet regularly and rest about a quarter (26.7%) users use Internet occasionally. So we find maximum people use Internet regularly. Table 7 explains the reasons for using Internet. We found that more than three out of five (66.7%) users use Internet in various purposes like e-mail, chat, browsing, seeking information and many more. Less than a quarter (13.3%) users use Internet for study purpose only and 16.7% users use Internet for their job purpose. From table 8 we see that, more than half (56.7%) users owned land phone at their home among young Internet users. The rest 43.3% have not any land phone at their home. In table 9 it is seen, less than a quarter (23.3%) users assess in tempting offer at the different web site(Case-1,3) and more than three out of five (76.7%) do not access to these attractive websites. Among the people who gave information at different tempting websites (Case-1&3), more than a quarter (28.6%) people gave their name and address, 14.3 % people gave their personal details, address and bank information. More than half of the people among those gave their details to that tempting websites (57.1%) (Table: 10). Among those people who didn't give any information to tempting websites more than half (60.9%) people don't believe this kind of covetable offers, a very few percent (8.7%) don't understand these offers and more than a quarter (30.4%) people have told that they did not do it without any reason (see table 11). From table 12 we get more than half (60%) young Internet users use online banking for their money transactions. And around 40% users have no account at any online bank. So, it can be said that, more people use online banking for their banking solutions. Among the 60% online banking users no one lost any money because of financial fraud. From table 13, we get, no one suffered from by any religious, political harassment. Specifically, in table 14 we found no one get any threat form others through e-mail. In table 14 we can see that a very few incidents like hacking occurred in Sylhet city, only 1 person suffered this kind of cybercrime but most of the people that is about 96.7% people don't affected by hackers. Among the young Internet users of cybercafés in

Sylhet city, 70% have personal computer at their home (table 15; Case-1, 2, 3, 5) and 30% have no personal computer. 95.2% computer owner reported that their computer affected by various viruses (table 16; Case-1, 2, 4, 5) and also told the main barrier of virus is thumb drive (table 16; Case-1, 4, 5). Only 4.8% users are free from virus attack. Among the victims of virus, 19% told that their computer attacked by virus in few times, 9.5% told average attack and 71.4% users told they are victimize lots of time because of virus and sometime they lost some valuable data and faced windows corruption because of viruses (see table 17). People who use computer at home generally (76.2%) use anti-virus software for their PC protection. Rest 23.8% people don't use any anti-virus for their PC to prevent unwanted occurrence. Among the PC owners who use anti-virus software for their PC 31.3% owner update their PC anti-virus regularly (Case-4) for better protection of their PC and most of the owners don't update their PC anti-virus regularly.

We find 3.3% users told us that their information leaked out in Internet and maximum (96.7%) users told they didn't found that their information leaked out in Internet (table 18). From table 19 we can see that 70% people gave their detail information to any social websites and 30% didn't log to that websites. In table 20 we get 95.2% people among social website's browsers gave their true information to those sites and 4.8% told they put fake information because of their information safety. From table 21, it is seen, maximum people (80%) told us that it is not fruitful to give any personal information to unreliable websites and 20% people think it may be a good chance to check luck because they thought they have nothing to lose by giving their information to tempting websites.

5. Conclusion

From the research we got the maximum Internet user are student (Table 4) and they use for their study purpose and many more. So we can say that in Sylhet the Internet user are limited in student community because, to use internet a person has to be knowledgeable about computer operation. We find few people gave their details to some tempting offers (Table 9). It is very interesting that who gave information to those sites thought that the offer is fake but they can not imagine that someone has stolen their identity. Among the respondent most people have no intention to get any thing by different tempting offer because they thought it's not for them, may be they can't afford that or something else.

We got more than half (56.7%) (Table 8) Internet users owned land phone but they did not victimize through theft of telecommunication service. There is more than half (60%)(Table 12) users use on-line banking that's mean on line banking is going to popular to young people because of its easy access but yet now no one lost any money through financial fraud. So we can say that because of rising on-line banking facility we should develop the consciousness about such type of cybercrime to save our nation's money. We find that the practice of e-mail threat, neglecting message about religion, political parties etc doesn't start here yet so no one has any experience about that. We know hacking is now most useable concept in cybercrime topic but in Sylhet district accept 1 respondent no one has that bad experience but we can't say that no hacking occurred in this cyber area because most of time users can't identify that he/she has been hacked by others. We see among the respondent more than three out of five (70%) (Table 15) people owned personal computer at their home and people use Internet who has no computer at home. It is clear that most of the people keep in touch with Internet so it is a good site of technological advancement. Most of the respondents reported that different types of virus affect their PC and they lost lots of valuable data and sometimes windows crash occurred. Most of the users use anti-virus software for virus protection but among them 68.8% computer owner don't update anti-virus so their attempt of prevent virus is practically doesn't work properly because everyday new viruses introduce in cyber world. So if they only use anti-virus without updating that will be fruitless and maximum users do that. We find 70% respondents gave their information to different social websites like www.facebook.com, www.hi5.com etc. Users said that they put the correct information on these websites but we know at present some hackers break down these websites protocols and can theft lots of information of different people and it is being doing now. So because of hacking of these sites general people may suffer for losing identity and it can occur without user's activity.

Therefore, it can be said that the young Internet users in Sylhet city don't affect by different cybercrime accept computer misuse but we can't say that most users are so conscious about the cybercrime. We find that most of the people have little idea about cybercrime and because of that they can't identify their position in Cyber world. In present world, third world countries are more choiceable to cybercriminals because they can do cybercrime here easily. So, as staying at the first stage of the network world, government should perform some activities to make people conscious about cybercrime. If we reduce the affect of cybercrime in our country that will be a great achievement for us, and this success not for the peoples only it's for the nation. Now it's the time to come forward and enter into the digital world with full protection and safety.

References

ACPR. (2006). *Parliamentary joint committee on the Australian crime Commission.* Retrieved from http://www.acpr.gov.au./pdf/ACPR145_2.pdf

ACPR. (2006). *Standardisation of definitions of identity crime terms: A step towards consistency.* Retrieved from http://www.acpr.gov.au./pdf/ACPR145_3.pdf

Baker, T. L. (1994). *Doing Social Research* (2nd ed.). Mc Graw-Hill, Inc, Singapore.

Blindell, J. (2006). *Review of the legal status and rights of victims of identity theft in Australasia.* Retrieved from http://www.acpr.gov.au./pdf/ACPR145_2.pdf

Borhanuddin, A. R. M. (2006). *Cybercrime and Bangladesh perspective.* Retrieved from http://www.scribd.com/doc/3399476/cyber-crime

Brenner, S. W., & Goodman, M. D. (2002). Cybercrime: The Need to Harmonize National Penal and Procedural Laws. Retrieved from http://www.isrcl.org/paper/brenner.pdf

Convention on Cyber-Crime. (2001). *The Convention on Cyber- Crime, a unique instrument for international co-operation.* Budapest: Council of Europe. Retrieved from http://conventions.coe.int/treaty/EN/projets/projets.htm

El-Guindy, M. N. (2008). *Cybercrime in the Middle East.* Retrieved from www.cybercrimejournal.co.nr

Etter, B. (2002). *Cybercrime: now this changes everything!* Retrieved from http://www.acpr.gov.au/pdf/presentations/netalertdec02.pdf

Fafinski, S. (2008). *UK Cybercrime report* Retrieved from http://www.garlik.com

Gjata, O. (2007). *Cybercrime.* Retrieved from http://mason.gmu.edu/~ogjata/index.html

Graycar, A. (2000). *Nine types of cyber crime.* Retrieved from http://aic.gov.au/conference/other/graycer_adam/2000-02-cybercrime.html

Hammadi, S. (2008). *A click away from crime.* Retrieved from http://www.prp.org.bd/Media/14-20March08.pdf

Hossain, A. (2004). *Access to Internet: Bangladesh Perspective.* Retrieved from http://www.mosict.gov.bd

Kowalski, M. (2002). *Cyber-Crime:Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics.* Catalogue No. 85-558-XIE, ISBN 0-660-33200-8. Retrieved from http://statcan.gc.ca/pub/85-558-x/85-558-x2002001-eng.pdf

Morris, S. (2004). *The future of netcrime now: Part 1 - threats and challenges.* Retrieved from http://www.homeoffice.gov.uk/rds/pdf04/rdsolr6204.pdf

Nachmias, & Nachmias. (2002). *Research Methods in the Social Sciences.* St Martin Press Inc. Fifth Avenue, New York, NY-10010.

Reynolds, P. D. (1976). *A Primer In Theory Construction.* The Bobbs-Merrill Company, Inc.

Seigfried, K. C., Lovely, R. W., & Rogers, M. K. (2008). *Self-Reported Online Child Pornography Behavior: A Psychological Analysis.* Retrieved from http://www.cybercrimejournal.co.nr

Young, K. (2008). *International journal for cyber criminology.* Retrieved from www.cybercrimejournal.co.nr/

Appendix 1. Tables

Table 1. Age of respondent

Category	Frequency	Percent	Modal category
18-22	10	33.3	
23-26	12	40.0	23-26
27-30	8	26.7	
Total	30	100.0	

Table 2. Sex of respondents

Category	Frequency	Percent	Modal category
Male	28	93.3	
Female	2	6.7	Male
Total	30	100.0	

Table 3. Educational status

Category	Frequency	Percent	Modal category
SSC	1	3.3	
HSC	7	23.3	
Honours	16	53.3	Honours
Masters	6	20.0	
Total	30	100.0	

Table 4. Occupation of respondent

Category	Frequency	Percent	Modal category
Student	19	63.3	
Service holder	5	16.7	
Private service	5	16.7	Student
Unemployed	1	3.3	
Total	30	100.0	

Table 5. Duration of use internet

Category	Frequency	Percent	Modal category
1 -3	10	33.3	
4 -6	12	40.0	4-6
7 -10	8	26.7	
Total	30	100.0	

Table 6. Regularity of use

Category	Frequency	Percent	Modal category
Yes	22	73.3	
No	8	26.7	yes
Total	30	100.0	

Table 7. Reason of internet use

Category	Frequency	Modal category
Study	4	13.3
Job	5	16.7
Various purpose	20	66.7
Private	1	3.3
Total	30	100.0

Table 8. Owning land phone

Category	Frequency	Percent	Modal category
Yes	17	56.7	
No	13	43.3	Yes
Total	30	100.0	

Table 9. Giving information at any offer in internet

Category	Frequency	Percent	Modal category
Yes	7	23.3	
No	23	76.7	No
Total	30	100.0	

Table10. Types of given information at any tempting offer

Category	Frequency	Percent	Modal category
Name and address	2	28.6	
1 and bank account information	1	14.3	
Additional information	4	57.1	Additional information
Total	7	100.0	

Table 11. Reason of not giving information

Category	Frequency	Percent	Modal category
Don't believe	14	46.7	
Don't understand	2	6.7	
No reason	7	23.3	Don't believe
Total	23	76.7	

Table 12. Use online banking

Category	Frequency	Percent	Modal category
Yes	18	60.0	
No	12	40.0	Yes
Total	30	100.0	

Table 13. Any neglecting message in internet

Category	YES	NO	TOTAL
Getting erotic info about yourself	0	30	30
Getting threat through e-mail	0	30	30
Neglecting message about religion	0	30	30
Neglecting message about political ideology	0	30	30

Table 14. Affected through hacking

Category	Frequency	Percent	Modal category
Yes	1	3.3	
No	29	96.7	No
Total	30	100.0	

Table 15. Owning a computer

Category	Frequency	Percent	Modal category
Yes	21	70.0	
No	9	30.0	Yes
Total	30	100.0	

Table 16. Affected through virus

Category	Frequency	Percent	Modal category
Yes	20	95.2	
No	1	4.8	
Total	21	100.0	Yes

Table 17. Times of virus attack

Category	Frequency	Percent	Modal category
Few	4	19.0	
Average	2	9.5	
Many	15	71.4	Many
Total	21	100.0	

Table 18. Disclose information of respondent

Category	Frequency	Percent	Modal category
Yes	1	3.3	
No	29	96.7	No
Total	30	100.0	

Table 19. Access Social Websites

Category	Frequency	Percent	Modal category
Yes	21	70.0	
No	9	30.0	Yes
Total	30	100.0	

Table 20. Putting correct information

Category	Frequency	Percent	Modal category
Yes	20	95.2	
No	1	4.8	Yes
Total	21	100.0	

Table 21. Mentality about the web offers

Category	Frequency	Percent	Modal category
Yes	6	20.0	
No	24	80.0	No
Total	30	100.0	

Appendix 2. Case Studies

Case 1

Name: Mamun (Pseudo name)

Age: 23

Occupation: student

Family particulars

Mamun is the student of honors 3rd year at M C college, Sylhet. His father is a government service holder. His mother is a housewife. He has 1 brother and no sister. His brother is studying in class eight.

Mamun said about cybercrime,

> "Basically I have no broad idea about cybercrime. I have been using Internet for 3 years. Generally I use Internet for study purpose but I do chat, browsing and other activities what I like at browsing time. I am very curious about to know something new. One I got an e-mail that a old lady wants to help the deprived children but she is unable to do this because of her some problem so she wants someone who can build up her dream. 1st time I thanked her and told my limitations. She told me that if I try that I can do something for the children and the amount of money is $7.5 million. After this big amount I agreed with her and by sequence she took my particulars and after 3 or 4 mails she gave me a lawyer's address and told me to contact with him for legal transfer of money. The lawyer asked me $3000 for transferring money. Than I talked to my friends about that and he told me that they are fraud. After that I told them I will give twice after the money and from than they stopped e-mail. I bought computer 3 years ago. I faced huge problem for viruses. The virus spread by thumb drives. I use antivirus software but I don't update it regularly. I think if any person takes money from other by credit card its called cybercrime".

Case 2

Name: Ifty (Pseudo name)

Age: 19

Occupation: student

Family particulars

Ifty is the student of honors 1st year at M C College, Sylhet. His father is a businessman. His mother is a schoolteacher. He has 1 brother and a sister. His brother is studying in class eight and sister studying at class 4.

Ifty said about cybercrime,

> "I heard cyber crime but I have no details idea about it. I have been using Internet for 2 years. I use Internet in various purposes. Basically I use e-mail more. I am so weak in English so I can't understand everything in Internet. I didn't put any information about me to any website because I like to browse only. I have a computer and I faced virus problem many times. I re-installed windows 2 times because of virus. I can't remove virus. Sometime my best friend helps me for maintaining the computer. I just use computer nothing else. I think credit card fraud is a cybercrime".

Case 3

Name: Raju (Pseudo name)

Age: 27

Occupation: Business

Family particulars

Raju is a businessman. He is married. His wife is a housewife. He has no children.

Raju said about cybercrime,

> "I know the term cybercrime but I can't explain it properly. I use Internet for 5 years but I do not use regularly. I got an offer in Internet for the green card of USA. I logged here and gave my details and they told me that I am qualified for the visa. I was so happy to hear that but they demand $6000 for visa processing but I had no enough money to give them that's why I stopped it here. I do believe it was really a good offer what I couldn't afford. I have no computer at my home but I'll get it soon. I think any crime occurred in Internet is cybercrime".

Case 4

Name: Sumon (Pseudo name)

Age: 23

Occupation: student

Family particulars

Sumon is the student of honors 3rd year at SUST, Sylhet. His father is a Private Service holder. His mother is a housewife. He has 2 brothers and 1 sister. His brothers are studying in class eight and class six. His sister is married and not stays with them.

Sumon said about cybercrime,

> "I have little idea about cybercrime. I use Internet for 4 years at my SUST lab. I use Internet for seeking information, e-mail, face book etc. I accessed lots of offer in Internet but I didn't give my true details here because I know it's not true and it's a way of virus attacks. I do it at SUST lab but not my PC. I use anti-virus software for my PC and try to update it regularly but it wouldn't be possible for every moment. My PC attacked by virus few times and the main reason of virus is pen drive. If you download something at cybercafé and want to bring it to self PC than it is must that you'll bring virus with your files. Many times virus is not so harmful but sometime it crashes the computer windows. I think any activities against law of cyber space are cybercrime".

Case 5

Name: Shafiq(Pseudo name)

Age: 28

Occupation: private service holder

Family particulars

Shafiq is a service holder of private TV channel. He is married. His wife is a student of Honors 3rd year. He has

no child.

Shafiq said about cybercrime,

> "I know nothing about cybercrime. I just use Internet for sending news to my higher authorities through e-mail. I have no curiosity about Internet. I just do it for my profession. I have a dextop computer at my home. I use it for making news. My PC affected many times for computer virus and these viruses come by pen drive form cybercafé where I use Internet. I use an anti-virus but don't update it. I found this anti-virus couldn't detect all viruses. I think any crime occurred by computer is cybercrime".

Appendix 3. Figure Representations

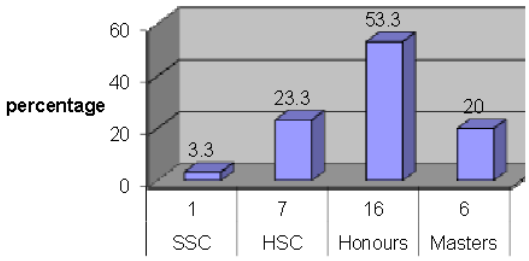


Figure 1. Educational qualification of respondents

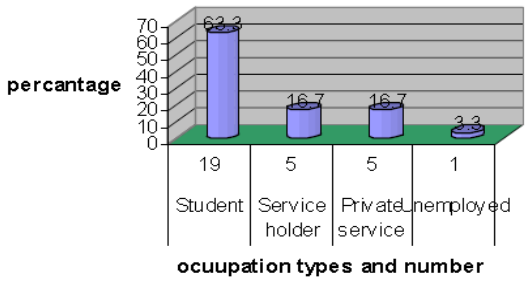


Figure 2. Occupation of the respondent

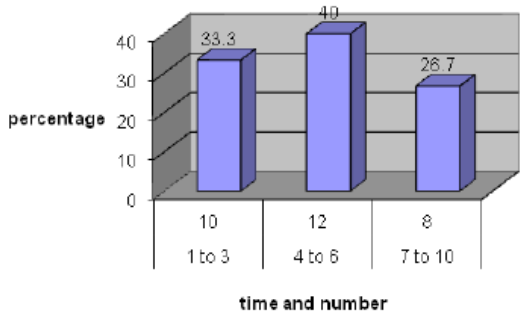


Figure 3. Duration of internet use

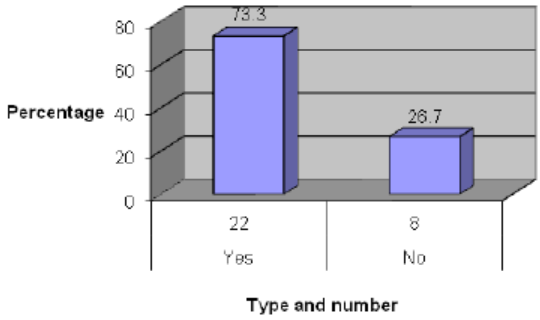


Figure 4. Regularity of internet use

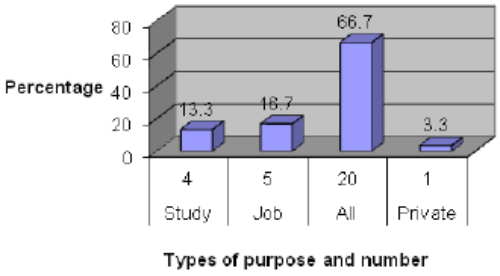


Figure 5. Purpose of use internet

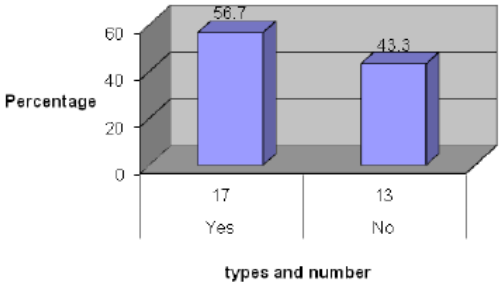
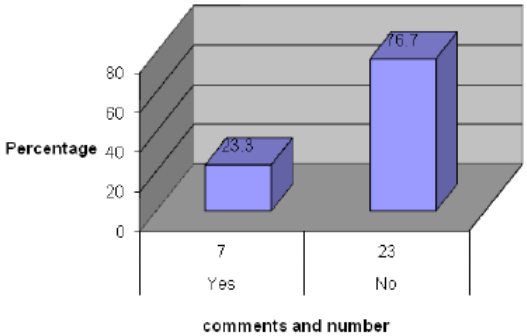


Figure 6. Owning land phone



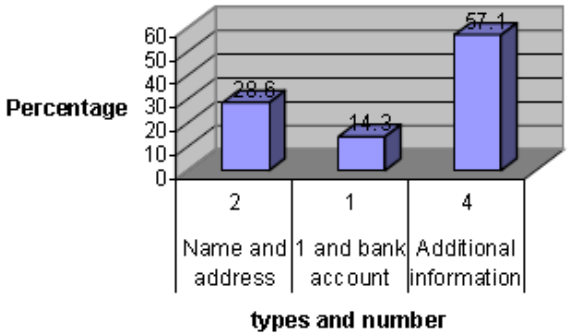


Figure 7. Giving information at any offer in internet

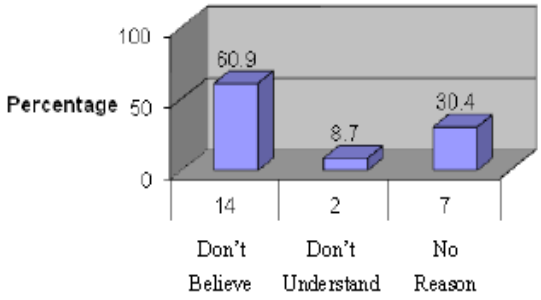


Figure 8. Types of given information

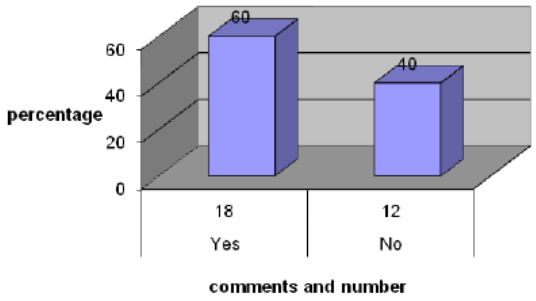
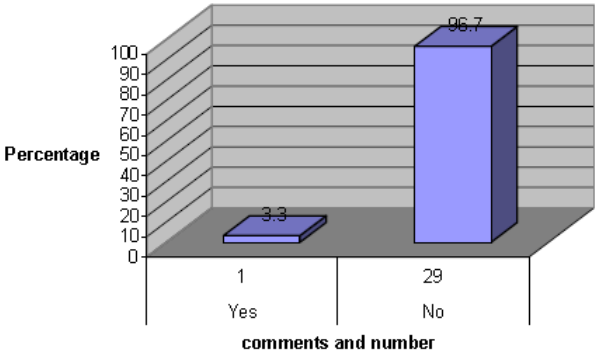


Figure 9. Reason of not giving information

Figure 10. Use on line banking



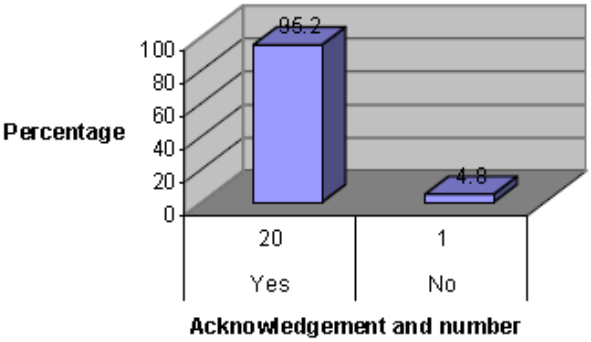
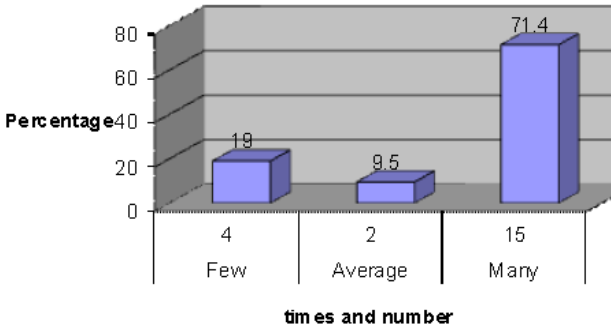


Figure 11. Affected through hacking

Figure 12. Affected through virus



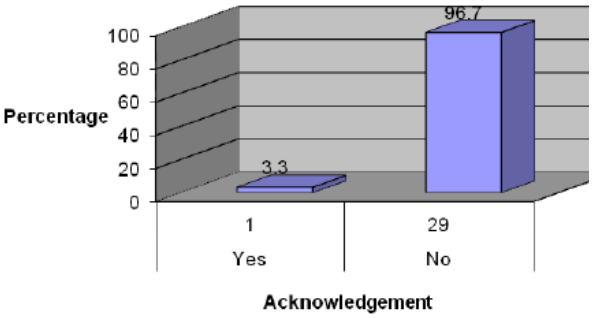
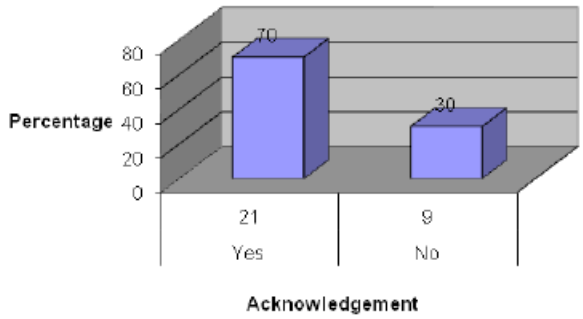


Figure 13. Times of virus attack

Figure 14. Disclose information



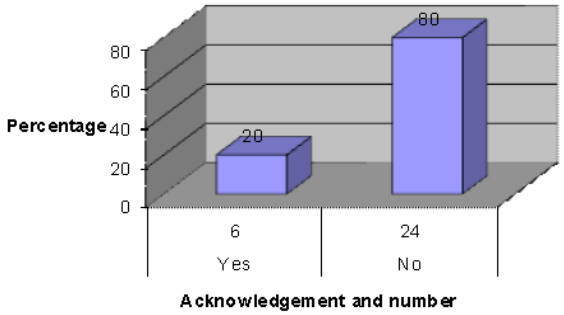


Figure 15. Access social website

Figure 16. Mentality about web offers