Research Article

BIOMEDICAL Journal of Scientific & Technical Research

ISSN: 2574 -1241

DOI: 10.26717/BJSTR.2023.52.008270

Pattern of Cybercrime among Adolescents: An Exploratory Study

Mohammad Shahjahan[1]* and Md. Abdul Kader Miah[2]

[1]*Director (Research & Publication), Police Staff College Bangladesh, Bangladesh*

[2]*Associate Professor, Department of Criminology and Police Science, Mawlana Bhashani Science and Technology University, Bangladesh*

***Corresponding author:** Mohammad Shahjahan, Director (Research & Publication), Police Staff College Bangladesh, Bangladesh

ARTICLE INFO

Received: August 18, 2023

Published: August 29, 2023

Citation: Mohammad Shahjahan and Md. Abdul Kader Miah. Pattern of Cybercrime among Adolescents: An Exploratory Study. Biomed J Sci & Tech Res 52(3)-2023. BJSTR. MS.ID.008270.

ABSTRACT

Background: Cybercrime is common phenomenon at present both developed and developing countries. Young generation, especially adolescents now engaged internet frequently and they commit cybercrime frequently in Bangladesh.

Objective: In this regard, the present study on the pattern of cybercrime among youngers of Bangladesh has been conducted.

Methods and tools: This study was a cross-sectional study, descriptive in nature. Non-probability accidental sampling technique has been applied to select the sample because of the nonfinite population and the sample size was 167. A printed semi-structured questionnaire was used to collect data.

Results: The study shows that adolescents mainly do hacking (94.6%), pornography (88.6%), software piracy (85 %), cyber theft (82.6%), credit card fraud (81.4%), cyber defamation (75.6%), sweet heart swindling (social network) (65.9%) etc. as cybercrime. According to findings the major causes of cybercrime among the respondents in Bangladesh were- weak laws (88.0%), defective socialization (81.4%), peer group influence (80.2%), easy accessibility to internet (74.3%), corruption (62.9%), unemployment (58.7%), and poverty (24.6%) etc. It is evident from the study that 91.0% respondents used password cracker as the techniques of cyber criminality. About 76.6%, 72.5%, 71.9%, 68.3% and 60.5% respondents' technique was key loggers, network sniffer, exploiting, vulnerability scanner and port scanner consecutively.

Conclusion: The study concluded that pattern of cybercrimes is frequently changing and increasing dramatically. Finally, it is recommending that the private public partnership and execution of existing laws can be controlling this crime.

Keywords: Cybercrime; Adolescents; Pattern; Internet

Introduction

Globalization process and development of the modern civilization led to the transition of industrial society to information society and introduction of modern information technologies creates new, unique opportunities for more active and efficient development of economy, politics, country, society, social consciousness, and a citizen [1]. 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. With the improvement of technology, approximation is that majority of these adolescents 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 young people are more exposed to cyber activity than their guardians, the cultural gap is there and exposing the young age people into a new dimension of global world. Communication has become one of the most

crucial integration ways in the world. It has changed 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. Moreover, it is true that teenage age is the dangerous age for human life. In this age, people choose their moral level of personality at teenage age what he/she is learning from their environment & what they will be about moral & character personality. In Bangladesh, age 13-18 years is the most dangerous age which may be considering as a teenage age. It is the turning point for them. Later, it is quite impossible to alter themselves after teenage age but possible with low success rate. Under such circumstances present study is going to inquiry the present scenario among the young people (13-20 years) about the extent and nature of cyber accessibility and its coherence to cybercrime.

Methods

Research aims to help or solve problems and investigate relationships of the numerous variables that exist around us. As an investigative process, research takes place at different levels of scientific sophistication. The present study on the pattern of cybercrime has been conducted in Dhaka City in Bangladesh. Explorative research design has been used in this research to explore the real situation of cybercrime among the teenagers in this area. The population of this research was not finite because internet users in cybercafés and other places could not be counted. So, people who use internet (age group 13 to 20 years) have been counted at several sites 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 167. The area of Dhaka city was clustered based on the geographical distribution which is as follows:

A. Dhaka North

i. Education Zone-01: Uttara, Gulshan, Banani and surrounding areas [40 samples/respondents (10 of each area)]

ii. Education Zone-02: Mirpur, Tejgaon, Mohamadpur and surrounding areas [40 samples/respondents (10 of each area)]

B. Dhaka South

i. Education Zone-03: Dhanmondi, Lalbagh, Shyampur and surroundings areas [40 samples/respondents (10 of each area)]

ii. Education Zone-04: Ramna, Motijhell, Demra and surrounding areas [40 samples/respondents (10 of each area)]

In this way, (40x4) =160 samples/ respondents were being counted but for availability of data extra 7 sample/ respondents had been included with the existing sample. So, the total number of samples was counted as (160+7) =167. Both primary and secondary sources of data/in formations were used in the research. The primary data for this study were collected directly from field by using an interview schedule, which contained both structured and open-ended questions. The interviewer asked the questions and recorded their answers. The secondary data were mainly complied through searching the available literatures and mostly used as the supporting materials in considerations of better presentation of the study. Data have been collected through social survey (face to face interview with questionnaire). After collecting data, simple statistical tools like univariate analysis; percentage distribution have been used to analyze data. Here SPSS version 20 is used in analyzing the collected data (Figure 1).

Figure1: Class wise percentage composition of zooplankton in Samrat Ashok Sagar.

Results

Table 1 has extended the types of cybercrime performed by the adolescents in Bangladesh. The results shows that 94.6% respondents were involved in hacking, 88.6% in pornography, 85.0% in software piracy, 82.6% in cyber identity theft, 81.4% in credit card fraud, 75.6% in cyber defamation, 73.1% in malicious program/ virus dissemination, 67.1% in cloning of website, 65.9% in sweetheart swindle (social network) and 15.6% in other types of cybercrime related activities, like stalking, publishing erotic materials etc. Causes of cybercrime among adolescents are shown in Table 2. Here it is seen that several causes are identified by the study subjects' like- weak laws (88.0%), defective socialization (81.4%), peer group influence (80.2%), easy accessibility to internet (74.3%), corruption (62.9%), unemployment (58.7%), and poverty (24.6%).

Table 1: Percentage distributions of the respondents by types of cybercrime.

Activity	Yes		No		Total	
	Number	Percent	Number	Percent	Number	Percent
Cloning of website/Phishing	112	67.1	55	32.9	167	100
Credit card fraud	136	81.4	31	18.6	167	100
Cyber defamation	126	75.6	41	24.6	167	100
Cyber identity theft	138	82.6	29	17.4	167	100
Cyber stalking	119	71.2	48	28.7	167	100
Hacking	158	94.6	9	5.4	167	100
Malicious program/ Virus dissemination	122	73.1	45	26.9	167	100
Pornography	148	88.6	19	11.4	167	100
Software piracy	142	85.0	25	15.0	167	100
Sweetheart swindle (Social network)	110	65.9	57	34.1	167	100
Others (specify)	26	15.6	141	84.4	167	100

Table 2: Percentage distributions of the respondents by causes of cybercrime.

Views	Agreed		Undecided		Disagreed	
	Number	Percent	Number	Percent	Number	Percent
Corruption	105	62.9	47	28.1	15	9.0
Defective socialization	136	81.4	24	14.4	7	4.2
Easy accessibility to internet	124	74.3	19	11.4	24	14.4
Peer group influence	134	80.2	26	15.6	7	4.2
Poverty	41	24.6	62	37.1	64	38.3
Unemployment	98	58.7	33	19.8	36	21.6
Weak laws	147	88.0	13	7.8	7	4.2
Others (specify)	8	4.8	13	7.8	146	87.4

Table 3: Percentage distributions of the respondents by techniques/tools of Cyber Criminals.

Techniques/tools	Yes		No		Total	
	Number	Percent	Number	Percent	Number	Percent
Exploit	120	71.9	47	28.1	167	100.0
Key loggers	128	76.6	39	23.4	167	100.0
Network sniffer	121	72.5	46	27.5	167	100.0
Password cracker	152	91.0	15	9.0	167	100.0
Port scanner	101	60.5	66	39.5	167	100.0
Vulnerability scanner	114	68.3	53	31.7	167	100.0
Others (specify)	13	7.8	154	92.2	167	100.0

(Table 3) The above table shows the techniques that were used by the respondents. It is evident that 91.0% respondents used password cracker as the techniques of cyber criminality. 76.6% respondents' technique was key loggers, 72.5% tools was network sniffer, 71.9% technique was exploiting, 68.3% adolescents' technique was vulnerability scanner and 60.5% used port scanner as a technique.

Discussion

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 all developed countries have taken steps to address the problem on the other hand developing countries are far away from being able to guarantee these rights. But Bangladesh Government has already shown its commitment to ICT through sharing the common vision of developing an Information Society, harnessing potential of ICT to promote development goals of the Millennium Declaration. Which includes eradication of extreme poverty and hunger, achievement of universal primary education and development of global partnerships for the attainment of a 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.

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 the cybercrime among the young people of Bangladesh was investigated at field level. The study found that adolescents mainly do hacking, pornography, software piracy, cyber theft, credit card fraud, cyber defamation, sweetheart swindling (social network) etc. as cybercrime. Kamal [2] describes the nature of cybercrime 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 cybercrime is not in serious condition in research area, the respondents were victimized sometime by hacker, pornography sites and computer virus through internet. It is continuously growing attention of the majority people of the study area.

Dutt, et al. [3] gives data regarding cybercrime, which is fast ever increasing in frequency and in acuteness, requires rethinking how should implement the criminal laws. The present model of reactive cybercrime, its types, modes of cybercrime and security measures including stoppage, deals effectively with cybercrime. It shows a requirement for a timely review of existing approaches to fighting this new phenomenon of cybercrime in the information technology. Though it is impossible to remove cybercrime from the world but can reduce it to a large amount by creating alertness in society. They suggested that a system of administrative regulation backed by criminal sanctions that will cater the incentives necessary to create a workable limiting to cybercrime. According to findings the major causes of cybercrime among the respondents in Bangladesh were- weak laws, defective socialization, peer group influence, easy accessibility to internet, corruption, unemployment, and poverty etc. Hassan, et al. [4] identified some of the causes of cybercrimes to include urbanization, unemployment, and weak implementation of cybercrime laws.

The effects of cybercrimes on organizations, society, and the country in general include reducing the competitive edge of organizations, waste of production time and damage to the image of the country. With Nigeria venturing into cashless society, there is a need for cybercrimes menace to be minimized if not completely eradicated. Some of the ways of combating such crimes include taking reasonable steps to protect one's property by ensuring that firms protect their IT infrastructure like networks and computer systems; government should assure that cybercrime laws are formulated and strictly adhered to, and individuals should observe simple rules by ensuring antivirus protection on their computer systems. It is evident from the study that 91.0% respondents used password cracker as the techniques of cyber criminality. About 76.6%, 72.5%, 71.9%, 68.3% and 60.5% respondents' technique was key loggers, network sniffer, exploiting, vulnerability scanner and port scanner consecutively. Okeshola, et al. [5] discussed the nature, causes and consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. In Nigeria today, numerous internets assisted crimes are committed daily in various forms such as identity theft, desktop counterfeiting, internet chat room, cyber harassment, fraudulent electronic mails, Automated Teller Machine spoofing, pornography, piracy, hacking, phishing, and spamming.

Usually, these crimes are committed in forms like sending of fraudulent and bogus financial proposals from cyber criminals to innocent internet users. Almost all the research work is some sorts of new and full of some new problems, for which it is needed to tackle some new thinking, new out looking as well as new understanding. It is recognizable that no research can be conducted without any problems or limitations. So, to do that during the study there were many problems to be faced. Firstly, the research work had to be completed within a limited period of time, and it was not possible to collect more in-depth information. Secondly, Lack of sufficient theoretical knowl-

edge on the proposed issue creates some problems to conduct this study properly or meticulously. Thirdly, as the respondents had no idea about the study, they were highly apprehensive about the purpose of the study. However, when they understood that the present study was academic, they were convinced and agreed to cooperate. Fourthly, several visits were made to get information. Despite these limitations, the study was conducted smoothly as had spirit and interest.

Conclusion

Cybercrime is new addition in criminology. In this study it is taken in consideration that Bangladeshi adolescents are engaged in various types of cybercrime somehow consciously and sometimes unconsciously and the situation is alarming. So, it is high time to make concentration about the matter both from related government agencies and community people.

Conflict of Interest

This was a self-funding study. There was no conflict of interest.

References

1. Golubev Vladimir (2005) Problems of counteraction to cybercrime and cyberterrorism in Ukraine. Computer Crime Research Center.
2. Kamal MM, Chowdhury IA, Haque N, Chowdhury MI, Islam MN (2003) Nature of Cyber Crime and Its Impacts on Young People: A Case from Bangladesh. Asian Social Science Archives 8(15): 171.
3. Dutt S, Suneyna, Chaudhary A (2013) Cybercrime: The Transition of Crime in the Information Era. International Journal of Advanced Research in IT and Engineering 2(6): 27-36.
4. Hassan AB, Lass FD, Makinde J (2012) Cybercrime in Nigeria: Causes, Effects and the Way Out. ARPN Journal of Science and Technology 2(7): 626-631.
5. Okeshola, Folashade B (2013) The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. American International Journal of Contemporary Research 3(9): 98-114.

ISSN: 2574-1241

DOI: 10.26717/BJSTR.2023.52.008270

Mohammad Shahjahan. Biomed J Sci & Tech Res

Submission Link: https://biomedres.us/submit-manuscript.php