Plight of Youth Perception on Cyber Crime in South Asia

Md. Kamruzzaman[1, 2, 4, *], Md. Ashraful Islam[1, 2], Md. Shahidul Islam[2], Md. Shakhawat Hossain[2], Md. Abdul Hakim[3]

[1]School of Victimology and Restorative Justice, Institute of Social Welfare and Research, University of Dhaka, Dhaka, Bangladesh
[2]School of Criminology and Police Science, Mawlana Bhashani Science and Technology University, Tangail, Bangladesh
[3]School of Food Technology and Nutritional Science, Mawlana Bhashani Science and Technology University, Tangail, Bangladesh
[4]School of Law, National University, Gazipur, Bangladesh

Abstract

Cyber crime is a buzzword all over the world. Due to the global connectivity and online activities it has become a global concern, not a territorial one and is spreading in a terrific volume. In this regard mostly the young people are in vulnerability and being victimized by various means. The study aim was to access these states in South Asian developing countries (i.e., the demographic subdivision Bangladesh). The descriptive type of cross sectional study was carried out to assess the perception, causes and consequence of cyber crime among youth using purposive sampling method taking a sum of 118 respondents from Tangail municipality and Dhaka north City Corporation areas in Bangladesh. The study found most of respondents (46.61%) belonged to age group 19 to 21 years and 66.10% were male while 60.16% were in vulnerability of cyber crime by Internet fraud and 78.81% agreed that social media increase victimization by dissemination of false information (55.08%). It also found Maximum respondents (82.20%) were affected by virus attack, 56.78% were secondary victimized while most of them (72.03%) felt unsafe in cyber space and 61.86% said awareness can reduce victimization.

1. Introduction

Computer brings a revolutionary change 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 data and information. We can get any information from the Internet world. Though it is the easiest way of communication, now it is the matter of concern that abuse of computer and Internet put together some people to commit crime and victimize others. According to Council of Europe "Any criminal offence committed against or with the help of a computer network is identified as cyber crime". So computer or computation related deviceis an essential for cyber crime perpetration and victimization [1].

Computer crime defined as criminal activities, involving information technology infrastructure, including illegal access of computer data from or within a computer [2]. Cyber crime is a worldwide problem now; no country is immune. 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

* Corresponding author
E-mail address: shohag.mbstu.cps@gmail.com (Md. Kamruzzaman)

world and in Middle East and third world countries the growth of Internetconnectivity in recent years increase in cyber criminal activities [3]. Fafinski's study asserts that in 2001 approximately 28.5 million people in the UK use the Internet [4]. Internet use in the Middle East had reached 2.5% of the total worldwide use by December 2007 [3].

Different nations have adopted different strategies to contend with crimes depending on their nature and extent. Certainly, a nation with high incidence of crime cannot grow or develop. For Bangladesha nation that is in the process of development facing problems regarding cybercrimes. In Bangladesh Internet was first introduced in 1996 [5]. 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 [6]. In another report says about 2 million people use Internet in Bangladesh [5]. Among this large number of people many people are being victimized by the devastating attack of cybercrime. Because of cybercrime people lost their money, identity and many more. News of media and status those posted in the social media are the exemplary evidence of victimization. Total number of cybercrime and victimization of cybercrime is not revealed in Bangladesh, but the condition of other countries can represent an overall image. In Canada by the year 2000 the 45,950 computer crimes reported by the NIBRS and noted that most common type of computer crime was larceny/theft [7]. 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 [8]. 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 [4]. 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 [9]. 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 2007and 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 [10] which make our life problematic. Therefore, the current study was conducted to assess perception of cyber crime, nature and

causes of victimization among youth in South Asian countries [11-14].

2. Materials and Methods

The study was a descriptive cross-sectional study conducted at purposively selected Tangail municipality and Dhaka north City Corporation areas in Bangladesh. There were taken a sum of 118youngfor the continuation of the study in full swing. A well-structured questionnaire was developed containing both the open and closed ended query along with observation to collect data interviewing the respondents in the study areas. The gained collected data was checked and further rechecked far away from the sample areas. The questionnaire was formed in order to gain the relevant information considering the dependent variables i.e., age group, level of education, residency, socio-economic contour and independent variable i.e., behavioural changing patterns during January 2013 to June 2014. The questionnaire was checked daily closing the field work, rechecked again after collecting all data and coded before entrancing into the computer technology. The data was edited if seeing any discrepancy (wrong entry, doubt entry etc.) and the data was processed to undergo statistical analysis using SPSS 16 windows program. Microsoft Word and Microsoft Excel were taken into consideration to focus the results using tabular, graphical and chart icon.

3. Findings of the Study

From the study it is found that most of respondents (46.61%) belonged to age group 19 to 21years while 66.10% were male and Religion of 92.37% were Islam (Table 1).

Table 1. Socio-demographic characteristics of the respondents (N=118).

Parameters	Frequency	Percentage
Age (years)		
16-18	43	36.44%
19-21	55	46.61%
22-24	20	16.95%
Sex		
Male	78	66.10%
Female	40	33.89%
Religion		
Islam	109	92.37%
Hindu	9	7.62%

Table 2. Cyber-crime victimization phobia of the respondents.

Parameters	Frequency	Percentage
Information Sourcesof cybercrime		
Radio	4	3.38%
Television	34	28.81%
Internet	27	22.88%
Newspaper	33	27.96%
Others	20	16.95%
Vulnerability of cybercrime types		

Parameters	Frequency	Percentage
Internet fraud	71	60.16%
Hacking	48	40.67%
Internet harassment	65	55.08%
Identity theft	41	34.78%
Virus attack	69	58.47%
E-mail bombing	36	30.50%
How use of social media increase victimization?		
Harassment from fake id	32	27.12%
misuse of profile information	23	19.49%
dissemination of false information	65	55.08%
harassment in chat room	30	25.42%
cheating by giving wrong information	34	28.81%
Fake advertisement	46	38.98%
And information theft by phishing	16	13.55%
Did you think that cyber socialization increased the victimization of cyber crime?		
Yes	93	78.81
No	18	15.25
Didn't know	7	5.93
Effect of victimization		
Primary	118	100
Secondary	67	56.78
Tertiary	45	38.14
Did you feel safe in cyber space?		
Yes	31	26.27
No	85	72.03
No comment	2	1.69
Is awareness about Internet can reduce the victimization of cyber crime?		
Yes	73	61.86
No	19	16.10
Didn't know/can't say	26	22.03

Table 2 presented that, 27.96% respondents got information of cyber crime from television while 60.16% were in vulnerability of cyber crime by Internet fraud and 78.81% agreed that social media increase victimization by dissemination of false information (55.08%). It also found

56.78% were secondary victimized and 38.14 were tertiary victimized while most of them (72.03%) felt unsafe in cyber space and 61.86% thought awareness can reduce victimization.

Table 3. Relationship between Repeat Victimization and types of cyber crime.

Types of cyber crime	Second time experience of respondents	Third time experience of respondents	More than third time experience of respondents
Internet fraud	39 (33.05%)	17 (14.40%)	10 (8.47%)
Hacking	13 (11.01%)	8 (6.77%)	0
Internet harassment	37 (31.35%)	23 (19.49%)	19 (16.10%)
Identity theft	11 (9.32%)	3 (2.54%)	0
Virus attack	84 (71.18%)	77 (65.25%)	67 (56.77%)
E-mail bombing	19 (16.10%)	6 (5.08%)	3 (2.54%)

Table 3 presented that, there is a strong relationship between repeat victimization and type of crime while for virus attack second time victimization were 71.18%, third time victimization were 62.25% and more than third time victimization were 56.77%. In Internet harassment second time victimization were 31.35%, third time victimization were 19.49% and more than third time victimization were 16.10%.

Table 4. Causes of victimization.

Internet Fraud (62)	Hacking (28)	Internet harassment (48)	Identity theft (24)	Virus attack (97)	E-mail bombing(22)
Trap of monetary profit/reward (9) 14.51%	Untrusted login (12) 42.86%	Chat in open chat room (14) 29.17%	Giving personal information to unauthorized sites (14) 58.33%	Unauthorized software, games download (50) 51.55%	Giving email ID to unknown people over Internet (5) 22.72%
Excuse for aid of helpless people (7) 11.29%	Clicking on unauthorized links of photo, video and games (9) 32.14%	By posting irrelevant comments in social media (10) 20.83%	Giving personal information to unknown person over Internet (10) 41.67%	Give access to unknown security software (16) 16.49%	Giving email ID to unauthorized sites (7) 31.82%
False job or task opportunity over Internet (40) 64.51%	Phishing by fake gift or award (7) 25%	By misusing personal photos and videos (16) 33.33%		Advertisement clicking (19) 19.59%	Open view of email ID in social media (10) 45.45%
Fake opportunity of abroad visa (6) 9.67%		Unrecognized messaging (8) 16.67%		Clicking on unauthorized links of photo, video and games (12) 12.37%	

Table 4 showed that, most of the respondents over the Internet were victimized by false job or task opportunity (64.51%), Online scammers play role with trap of monetary profit/reward (14.51%) over the Internet, 11.29% using excuse of aid for helpless people. 9.67% online fraud related

to the fake opportunity of abroad visa. Online email or untrusted communications over Internet were main reason behind visa fraud. Most of the victim of the hacking use untrusted login (42.86%) of various websites.
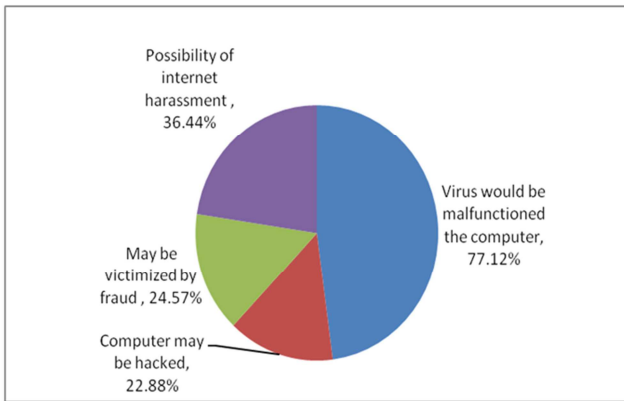
Figure 1. Types of fear felt in the case of cybercrime.

Cyber crime has deep impact on youth people. In most of the cases (77.12%) respondents fear that Virus would be malfunctioned the computer. In other cases they feel fear that their computer may be hacked (22.88%) or they may be victimized by fraud (24.57%) or they may be victimized by Internet harassment (36.44%) (Figure 1).
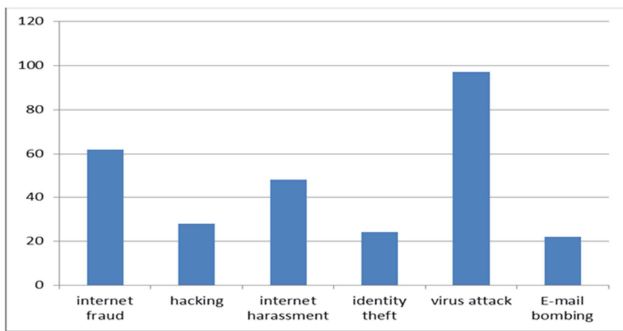

Figure2. Victimization of cybercrime.

Maximum numbers of the respondents (82.20%) are affected by virus attack, so virus attack is a common hazard for every Internet user while 52.54% victimized by Internet fraud, 40.68% were victimized by Internet harassment, 23.72% by hackingand 18.64% respondents were victimized by E-mail bombing (Figure 2).
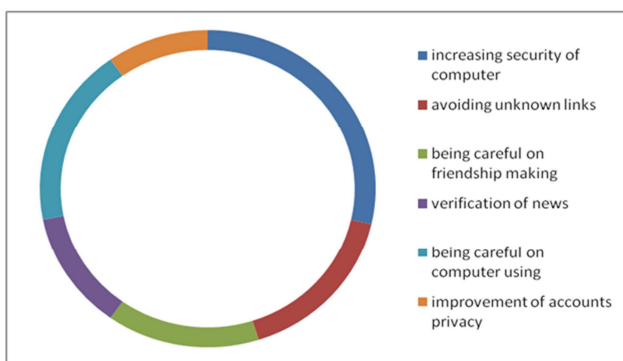

Figure 3. How awareness can decrease cyber crime victimization?

Figure 3 showed that 87.67% respondents gave emphasis on

increasing security of computer, 50.68% respondents said to raising awareness about avoiding unknown links, 45.21% for being careful on friendship making, 36.99% emphasized on verification of news, 56.16% for being careful on computer using, 30.14% emphasized on improvement of accounts privacy.

4. Discussion

Cyber crime victimization carries out unique reasons and impact upon youth people of the society. From the study it is observe that most of the respondents (83.05%) were teenagers, where majority of them were young male.

4.1. Usage, Vulnerability and Victimization

The study tried to find out that, is average day and duration have any impact on victimization. From the results it is explain that respondents those are victimized by cybercrime associated with Internet for much time. From the data 10.16% respondents use Internet for daily, 16.95% respondents use Internet in six days in a week and 28.81% respondents use Internet in five days in a week. In duration 10.16% respondents use Internet for above four hours, 14.40% respondents use Internet for four hours, 27.97% respondents use Internet for three hours. Password is a key security issue for any account. In most of the cases respondents use easy password that are direct threat to their account for hacking. In case of password 42.37% respondents use numerical number and 27.12% respondents use words. To understand the concept and reality the study tried to find out the perception of risk/vulnerability of cybercrime among respondents and real victimization of respondents. Respondents' perception about vulnerability of Internet fraud is 60.16%, where real victimization is 52.54%. Respondents were very much anxious about Internet fraud because they do not able to verify information over the web world. In the case of hacking 40.67% respondents feel risk where real victimization of hacking is 23.72%. Respondents fell more unsafe in cases of hacking because hacking can bring high amount of loss like id losing. In the perspective of Internet harassment 55.08% respondents feel unsecure where 40.68% are victimized by Internet harassment. The issues of Internet harassment quickly transmitted to the people and create instant fear of victimization. Risk or vulnerability of identity theft is 58.47%, where reality is 20.33%. Identity theft bring hazard for the real account holder and criminal can easily misuse the information or can use it for criminal activity. For that reason the impact of that crime bring the 58.47% sensitivity for identity theft. The interesting finding from the study is 82.20% respondents were victimized by virus attack but 58.47% respondents feel the risk of virus attack. Because respondents know that most of the time virus problem can be

easily solved with antivirus or preventive manner of use. In the case of email bombing vulnerability are 30.50% where real victimization are 18.64%. Respondents feel risk for email bombing because they got spam email more than past time. The study found more re-victimization in virus attack, Internet harassment and Internet fraud. In virus attack 71.18% respondents are victimized for second time, where 62.25% respondents are victimized for third time and 56.77% respondents are victimized for more than third time. On the other hand, 31.35% respondents are victimized by Internet harassment for second time where 19.49% are victimized by third time and 16.10% are victimized by more than third time. In Internet fraud 33.05% respondents were victimized for second time, where 14.40% respondents are victimized for third time and 8.47% respondents are victimized for more than third time which support another studies [15-20].

4.2. Causes of Cyber Crime Victimization

Experiences of cybercrime victimization in different cyber crimes have different victimizing reasons. Internet fraud is mostly affected by false or fake job or task opportunity (64.51%). Respondents get fake offer like online advertisement click job, task of like for social media pages, opening email accounts or fake offer of work as an employee of a renowned company. Online scammers play role with trap of monetary profit/reward (14.51%) over the Internet. They send scam mail for the trap or give phishing advertisement in the web pages. As a result people are losing their identity privacy or victimized by economic losses. In these cases, online fraudulent offenders are using public sentiment as a weapon. Victimization of hacking is enormously effected by untrusted login (42.86%) and clicking on unauthorized links of photos, videos and games (32.14%). Respondents are not aware about the untrusted access or too excited to explore new experience. In terms of Internet harassment misuse of personal photos and videos (33.33%) and chat in open chat room (29.17%) are main reason. Offenders misuse photos or videos of victim and upload those over the Internet. Identity theft is affected by giving information to unauthorized sites (58.33%) and person (41.67%). Young people easily give their personal information over Internet to download or see software, porn, game and photos. In the case of virus attack unauthorized software, games download (51.55%), fake advertisement clicking (19.59%) play vital role. Email bombing is being influenced by open view of personal information (45.45%) and giving email id to unauthorized people (22.72%) or sites (31.82%). Young people simply gave their personal email over Internet to get access in different web sites, but actually they find their way in a trap of world web which promotes victimization [21-24].

4.3. Cyber Socialization and Victimization

Use of social media is a common demand for each and every young people. In cybercrime victimization social media have crucial role. The study found that, 78.81% respondents are believed that cyber socialization have effect on victimization. In social media victims mostly affected by dissemination of false information (54.84%), fake advertisement (38.71%), cheating by wrong information (29.03%) and harassment (26.88%). Dissemination of rumour in social media gets quick coverage with sharing system. In social media anyone can open an account with wrong information. So offenders are easily able to misuse the benefit of identity privacy. They collect information of convenient target and misuse the open information of victims. Offenders also use emotional sentiments to achieve public support to spreading false information. Sometimes, offenders use social media for a medium of communication for physical criminal offences [25-29].

4.4. Effect of Cyber Crime Victimization

The effect of cyber crime victimization relies on primary, secondary and tertiary impact. All of the respondents are primarily victimized by cybercrime. Primary victimization contains monetary losses and psychological losses. Monetary losses includes costs of computer trouble shooting, theft of valuable information, fake job doing without pay and direct economic fraud victimization. Psychological losses include mental effect of private data losing, defamation and risk of re-victimization. On the other hand, 56.78% respondents believe that their family or institutions are the sufferer of his/her victimization where 38.14% respondents believed that community was victimized by the effect of cybercrime. Families of victims suffer from monetary losses or defamation or fear of victimization. Cases like identity theft bring losses of dignity and trust in the society. To understand the effect of cybercrime it is notable that, cybercrime increase significant magnitude of fear of crime than street crime. Security feelings about cyber space clarify the concept of victim about safety of web world. The study represent that, 72.03% respondents feel unsafe in cyberspace, where only 26.27% respondents feel safe in cyber space. Respondents who feel unsecure in cyberspace they feel fear of victimization for malfunction of computer for virus, hacking, fraud or harassment. Among them, victimization of virus attack (77.12%) and harassment (36.44%) create significant fear for young people. Increasing awareness about Internet use, Internet security and cyber crime can be helpful to decrease the fear of cyber crime [30, 31].

4.5. Role of Awareness in Cyber Crime Prevention

Cyber crime is an intrinsically human affair where one

individual tries to trick and exploit another. For that reason awareness can help to avoid those tricks. Generally, awareness programs are able to give basic knowledge about cyber space safety. For that reason 61.86% respondents believe that awareness in different areas decrease victimization. Awareness about computer security (87.67%), avoid unknown links (50.68%), careful computer operation (56.16%) are effective to decrease cybercrime. Computer security depends on use of antivirus or firewall. It is high time to take 1/n counselling to control this social, family, country to country cyber perils all over the world using the galore popular microsimulation modelling approach [32-34].

5. Conclusion

With the advancement of technology cyber crime is increasing day by day. In this, young people are victimized mostly for the sake of unawareness about cyber crime and its impact. They use Internet without proper security and verification which improves Internet harassment, hacking and also various criminal activities. In order to digitalize our country, there is no alternative to secure technological advancement among which tenable Internet using should prevail in priority. Along with raising awareness the law enforcement agencies and all stakeholders have to walk together to curve the modern perils like cyber crime.

References

[1] Shabnam N, Faruk MO and Kamruzzaman M (2016). Underlying Causes of Cyber-Criminality and Victimization: An Empirical Study on Students. *Social Sciences*, 5(1): 1-6.

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

[3] Frances, Umeozulu (2012) Perception of cyber crime among Nigerian Youths, Caritas University, Enugu.

[4] El-Guindy (2008). Cybercrime in the Middle East. ISSA. J.

[5] Fafinski, S (2008). UK cyber crime report.

[6] Kamruzzaman, M and Hakim MA. (2016). Livelihood Status of Fishing Community of Dhaleshwari River in Central Bangladesh. *International Journal of Bioinformatics and Biomedical Engineering*, 2(1): 25-29.

[7] Hossain, A. (2004). Access to Internet: Bangladesh perspective. From http://www.apdip.net/documents /evaluation/indicators/itu-bd16112004.ppt.

[8] www.crime-research.org/news/07.11.2007/2995.

[9] Kowalski, M. (2002). Cyber-crime: Issues, data sources, and feasibility of collecting police-reported statistics. Ottawa: Statistics Canada.

[10] Graycar, A. (2000) Fraud prevention and control in Australia. Paper presented at the AIC Fraud Prevention and Control Conference, Surfer's Paradise.

[11] Kamruzzaman M. (2015). Child Victimization at Working Places in Bangladesh, *American Journal of Applied Psychology*, 4(6): 146-159.

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

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

[14] Kamruzzaman M and Hakim M A. (2015). Child Criminalization at Slum Areas in Dhaka City, *American Journal of Psychology and Cognitive Science*, 1(4): 107-111.

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

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

[17] Kamruzzaman M and Hakim M A. (2015). Socio-economic Status of Child Beggars in Dhaka City. *Journal of Social Sciences and Humanities*, 1 (5): 516-520.

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

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

[20] Kamruzzaman M. (2015). Dowry related Violence against Rural Women in Bangladesh. *American Journal of Psychology and Cognitive Science*, 1(4): 112-116.

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

[22] Hakim M A and Kamruzzaman, M. (2015). Nutritional Status of Central Bangladesh Street Children. *American Journal of Food Science and Nutrition Research*, 2 (5): 133-137.

[23] Hakim M A and Kamruzzaman M. (2015). Nutritional Status of Preschoolers in Four Selected Fisher Communities. *American Journal of Life Sciences*, 3 (4): 332-336.

[24] Kamruzzaman M and Hakim M A. (2015). Family Planning Practices among Married Women attending Primary Health Care Centers in Bangladesh. *International Journal of Bioinformatics and Biomedical Engineering*, 1 (3): 251-255.

[25] Kamruzzaman M and Hakim M A. (2016). Factors Associated with the Suicidal Tsunami as a MentalIllness: Findings from an Epidemiological Study. *American Journal of Environment and Sustainable Development*, 1(1): 1-5.

[26] Kamruzzaman M and Hakim M A. (2016). Prostitution Going Spiral: The Myth of Commercial Child Sex. *International Journal of Biomedical and Clinical Sciences*, 1(1): 1-6.

[27] Das SK, Khan M B U and Kamruzzaman M. (2016). Preventive Detention and Section 54 of the Code of Criminal Procedure: The Violation of Human Rights in Bangladesh. *American Journal of Business and Society*, 1(3): 60-67.

[28] Kamruzzaman M. *et al.* (2016). Patterns of Behavioural Changes Among Adolescent Smokers: An Empirical Study. *Frontiers in Biomedical Sciences*, 1(1): 1-6.

[29] Kamruzzaman M and Hakim M A. (2016) Socio-economic Status of Slum Dwellers: An Empirical Study on the Capital City of Bangladesh, *American Journal of Business and Society*, 1(2): 13-18.

[30] Kamruzzaman M and Hakim M A. (2016). Condom Using Prevalence and Phobia on Sexually Transmitted Diseases Among Sex-Buyers in Bangladesh, *American Journal of Environmental and Occupational Health*, 1(1): 1-5.

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

[32] Rahman, A., Harding, A., Tanton, R. and Liu, S. (2013). Simulating the characteristics of populations at the small area level: New validation techniques for a spatial microsimulation model in Australia, *Computational Statistics and Data Analysis*, 57(1): 149-165.

[33] Rahman, A., Harding, A., Tanton, R. and Liu, S. (2010). Methodological issues in spatial microsimulation modeling for small area estimation, *International Journal of Microsimulation,* 3(2): 3-22.

[34] Hakim MA. (2016). Malnutrition Prevalence and Nutrition Counseling in Developing Countries: A Case Study. *International Journal of Nursing and Health Science*, 3(3): 19-22.