Journal of Society & Change
Vol. XIV, No.2, April-June 2020
ISSN: 1997-1052 (Print), 227-202X (Online)

Cybercrime: The Awareness of Secure Utilization of the Internet among the Students of Britannia University

Masum Bakaul[*]
Mahmuda Akter[**]

Abstract

Today the use of the internet has significantly increased for accessing and sharing information through the computer and other devices. The immense use of the internet and its dependence threaten user's confidential information due to increasing attempts by unauthorized third parties to break the security and gain access to the information for their own favor which is referred to as cybercrime. It is, therefore, essential for all users to understand the security mechanisms and potential risk factors of using the internet to protect their confidential information from unauthorized access. The paper focused on the study to investigate the awareness of cybercrime and cybersecurity in earning the harmless transmission of data and the secure use of the internet. The research is enriched with the findings through a questionnaire survey conducted over a period of three months where the targeted population (100) were the students of Britannia University. The data were analyzed using SPSS statistical software and the results have been shown using a frequency distribution table. It has been learned from the survey findings that a remarkable number of students (79%) possess good knowledge of cybercrime. The researchers also carefully explored whether the respondents have intentionally or unintentionally committed cybercrime or not. In the conclusion, the paper investigateswhether the precaution has been taken by the respondents against cybercrime and for secure usage of the internet. The authors recommended conductinga workshop and possible credit hours for creating awareness on cybercrime among the students and the necessary security mechanisms for making strong protection against this crime.

Keywords: Cybercrime, Cyber Security, Cybercrime awareness, Information Security, Secure Use of the Internet.

---

[*] Lecturer, Dept. of Computer Science and Engineering, Britannia University, Cumilla, Bangladesh, E-mail: masumbakaul.cse@gmail.com

[**] Student,Department Computer Science and Engineering, Britannia University, Cumilla, Bangladesh, E-mail: mafrin65@gmail.com

Introduction

Cybercrime is the combination of two words ‘cyber’ and ‘crime ‘where the word cyber came from the word Cybernetics. Possibly the word cybercrime has used at the end of the 1900s.Faisal (2016) described that cybercrime or computer crime is a form of crime here Internet or computer is the medium of crime. Cybercrime can be defined as a kind ofactivity that involves a computer, smart device, and network. Mia(2015) a Researcher define cybercrime as “Any criminal activity where either computer is an object or subject of conducting the crime”

The computer is the object of the crime used for hacking, phishing, spamming, or used as a tool to commit an offense like child pornography, hate crimes, and many more.While most cybercrimesare carried out in order to make money or profit, some cybercrimes are carried out against computers or devices directly to damage or gain access to confidential information for purpose of harm somebody, while others use computers or networks to spread malware, illegal information or other illegal materials. According to Watering (2019),the first person found guilty of cybercrime was Ian Murphy also known as Captain Zap and that happened in the year 1981. He had hacked the American telephone company to manipulate its internal clock so that people could make the free call at peak times.

Also in Bangladesh, the first cybercrime came to light in the nineteenth-century when there were probably around 30,000 internet users from the total population. According to Kamrul Faisal(2016),the first cybercrime case of Bangladesh was in 1995, the Secret Service and Drug Enforcement Agency (DEA) obtained the first Internet wiretap, which is exactly like a phone wiretap. Bangladesh is a developing country with a large number of populations in a small area and targeting to make Digital Bangladesh by 2021.People already walked into the era of digitalization.A large number of people are now using smart devices and the internet.The first internet service was launched in Bangladesh in the year of 1996.According to BRTC (2019) at the end of August 2019, the total number of users of the internet was 98.136 million which was 80.829 million at the end of January 2018 and 66.779 million at the end of January 2017 from the total population of the country.The user of the internet is increasing so fast.

With the growing amount of usage of the internet in Bangladesh, the frequency of cybercrime is increasing likein other countries of the world. According to Sarwar (2019), 3659 cases related to cybercrime has been lodged in Bangladesh over the last six years. The number of cybercrime cases was 233 in 2016,568 in 2017 then it ends up to 925 in 2018.In the first two months of 2019, 130 cases were filed. 34% of cybercrime victims were between the age of 19 to 25. Among the victims 53% were women and 47% were men.

But the matter of concern is with the increasing rate of cybercrime, awareness about cybercrime is not increasing alongside. As a result the students, business figures mainly the banks are being victimized by cybercriminals. Sharmeen Karim (2016) described that in February 2016 the largest e-money laundering in the history of banking occurred, hacker stole $101 million from Bangladesh Bank's account (p.16).In this scam, Dridex malware was used for the attack. It is not the only cyber-attacks in banks of Bangladesh. Hackers attacked other banks like Sonali Bank Bangladesh and stole a big amount of money. Hackers were able to hack those banks because of their weak access system in the SWIFT global payment network. A matter of big regret is that authority still couldn't find the culprit. Which is a big loss for a low-income country like Bangladesh.Sreehari et al. (2018) found that even though there are lots of security mechanisms against cybercrime but still people are far behind neutralized cybercrime because they are not aware of the impact.

Unawareness of cybercrime is one of the main obstacles to the improvement of our country. Cybercrime is the latest dangerous form of crime. It will terribly increase if the people stay unaware because only law is not enough to prevent its gruesomeness. Need to increase the security against it and the young generation must have to have proper knowledge about cybercrime, its impacts, and the security mechanism against the crimes.Shabnam et al. (2016) state a proper system is needed to build based on this era of cybercrime to protect the young generation from unwanted harassment (p.6).

Cybercrime in Bangladesh has been growing exponentially every few months. In this scenario, it is important for every single user of the internet and smart device to understand the potential risk and impact factors of not having enough knowledge of cybercrime and cybersecurity.Cybercrime is not an IT problem but it's a global problem. So, awareness of cybercrime is one of the major claims of recent time in Bangladesh actually all over the world.

Literature Review

Currently, it has identified cybercrime as a threat to the entire world. Over the past few years, Bangladesh has also faced cyber-attacks several times. Therefore, it is required to get the attention of a vast number of internet users in Bangladesh about cybercrime and its impacts. Several studies have attempted toBangladeshi studentsto determine the consciousness of cybercrime and the precaution they have taken to secure their confidential resources. Shabnam al. (2016) studyfound out of 54.9% of regular internet users 37.1% of students were conscious about cybercrime.Sarker and Shahid (2017) research found that 79.2% of the respondent use a mobile phone to access the internet.The present study

found similarities with Sarker research and has found 78% of respondents use mobile to access the internet. According to MostufaKamal et al. (2012a), 70% of the respondents spend time on Social media mostly.Ahmedet al.(2017), investigates that the womenfolk of Bangladesh faced cybercrime in social media most. A crime like bullying, harassment, fraud and he also said 73% of the women internet usershave faced cybercrime in social media.Kabir (2018) states in her research that cybercrime has increased in the banking sectors of Bangladesh since 2016. Banks are facing ATM fraud, E-money laundering, Credit card fraud, Phishing, etc.According to kumbar and Gavekar(2017),most of the respondents faced hacking and they change their login information frequently as a security measure.Sreehari et al. (2018) described that most of the respondents are not aware of cybercrime, they mostly aware of hacking compare to others and they were not worried about third parties data while online, they carried random web surfing overlooking the required security.According to Shabnam et al.(2016), due to a lack of knowledge on cybercrimes,fewerpeople lodged complain,and only a few complain had filled in the police station. A few of these complaints were properly justified as police still use the traditional method and they don't have the proper cyber-related skills as a result number of cybercrimes are increasing. Hanif(n.d.) states that to prevent cybercrime the ICT Ministry along with the IT expert and the media just needs to work together. And the authority should take legal action against the cybercriminal.CSI/FBI computer crime and security survey (2005), described people need to focus largely on technical issues like encryption, access control, detection system. The government should collaborate with the young generation and initialize proper steps on this serious matter to make them understand the consequences.

Purpose of the Study

1. To understand the awareness of cybercrime among the students of Britannia University.
2. To find out types of cyber-attack they have been facing.
3. To investigate whether respondents have been unintentionally involved in cybercrime or not.
4. To find out the precaution has been taken by the respondents for securing their confidential data from unauthorized access.

Methodology

The current study is empirical in nature with a combination of primary and secondary data collected from reliable sources. The primary data were collected from 100 respondents who were undergraduate students of

Computer Science and Engineering, Britannia University, through a random sampling method. A structured questionnaire with 26 items was used for data collection. The frequency distribution method in percentile was adopted to analyze the collected data to draw findings of the study using SPSS and MS Excel.

Findings

Table1.1: Respondents profile

Variable	Percentage
Gender	46% female, 54% male
Age	Age range 20-26. Average age 23-24

The study used a questionnaire survey as a major tool for collecting essential data. The respondents of the survey were university students and the total sample size was 100. The demographic of the respondents showed that a large percentage of the sample was male (54%) and the rest of them (46%) were female. The age group ranged from 20-26. Shabnam et al. (2018) claimed that there is a positive relationship between the person's characteristics and crime. Several studies found males are more involved in crime comparing to females and females were victimized more than males. Most of the time the underage person falls into crime more than the adult.

Table1.2: Finding's on the daily usage of internet

Daily user of internet	Percentage
Yes	95
No	5
Total	100

From the total population of 100 respondents, 95% said they use the internet on daily basis and 5% of respondents said they were not a daily user of the internet. The possibilities to become a victim of cybercrime can be detected from the daily internet using rate.

Table1.3: Comfortdevice's for internet usage

Gadget	Percent
Mobile	78
Laptop	15
Desktop	7
Total	100

In the fast-growing technological world, people are more dependent on different type's smart devices to accomplish their tasks. The studyhas been found the majority of the respondents(78%) use mobile to access the

internet. Sarker and shahid(2018) found similarity(79.3%)with our result (78%).15% of the total respondents uses laptop while 7% of them use desktop for web surfing. Respondents explained mobile is easier to carry and provides a simple interface to access the internet. As they spend plenty of time on the internet there are huge possibilities to become a victim or accused of cybercrime.

Table1.4: Perspectives of internet usage

Purpose	Percentage
social site	39.0
study material	17.0
movies	16.0
communication	28.0
Total	100.0

Internet is the blessings of this era. It is expected that university students should use the internet mainly for study purposesbut unfortunately, authors found mostly they spend their time on different social media and interactions based web sites.Out of 100 respondents, 39% ofstudents use the internet for social media and only 17% of them usethe internet for study purposes. They spend less time (16%) watching movies. Researchers also found a good number of students (28%) utilize the internet for communications purposes. Our study is in agreement with Kundu et al.'s (2018) study as they found social media is a big platform to fall into cybercrime.

Table1.5: Respondentscybercrime knowledge

Cybercrime knowledge	Percentage
Yes	79
No	21
Total	100

Table 5.5 discloses that 79% of respondentsaccumulated good knowledge on cybercrime and 21% said they don’t possess enough knowledge on cybercrime. But it is really difficult to ensure the actual knowledge of cybercrime as this criminology is a new concept and its variation in doing crime made it difficult to detect. In this table authors directly asked whether the respondents have knowledge of cybercrime and later in table 5.7 a deep analysis was performed to check whether they really carry the actual knowledge of cybercrime.

Table1.6: Cyber-attack experiences as a victim

Types of cyber attack	Percentage	
	Yes	No
Hacking	36	64
Identity Theft	25	75
Phishing	12	88

Computer Virus	21	79
Spamming	10	90
Cyberbullying	24	76
Pornography	24	76
Fraud	16	84

Table 5.6 described different types of cyber-attacks that the respondents have experienceslike hacking, identity theft, phishing, computer virus, spamming, cyberbullying, pornography, and fraud. From their given information it has been found that 12% have faced phishing which is a form of fraud. Attacker masquerades as a reputable entity in an email or other communication channel and gains access to the secret information.25% of them faced Identity theft while 24% have faced cyberbullying which is a form of bullying someone using digital devices.Several studies were carried out to explore the cyberbullying experiences among the students which have revealed male students were more involved in cyberbullying compared to female. Very little research has been carried out in Bangladesh regarding online cyberbullying that the students face today in a regular fashion. 24% of them faced pornography while 16% of respondents said they often faced hacking and fraud online.21% faced different virus attackson their computer.The lowest number of respondents (10%)have faced spamming, in spamming attackers use emails and sends malware and fake links to attract the user.

Table1.7:*Respondents actual knowledge of cybercrime*

Cybercrime	**Percentage**	
	Knowledgeable	**Inadvisable**
Hacking	61.4	38.6
Identity Theft	56.4	43.6
Phishing	27.5	72.5
Computer Virus	87.4	12.6
Spamming	20.5	79.5
Cyberbullying	63.6	36.4
Pornography	90	10
Fraud	60.4	39.6

Table 5.5 showed 79% of the respondents claim themselves as knowledgeable about cybercrime. In this table, researchersinvestigate their actual knowledge of cybercrime. The studyfound that respondents havea good command of hacking, computer virus, cyberbullying,identity theft, fraud, and pornography but a fairly limited number of respondents knows about phishing and spamming. This table examines a few dis-similarities with the respondent's opinion in table 5.5. Sreehari et al. (2018) also found in theirresearch thatonly a few internet users are conscious of cybercrime and most of the respondentswere not aware of their online information safety which is quite similar to ourstudy.

Table1.8:*Preventive measure was taken by the respondents*

Security mechanisms	Percentage
Installed anti-virus	49.3
Deleted social media app or acc.	1.6
Increased security on website	5
Update password	30
Only open known mail	7
Only accept and chat with the known person online	7.1

Table 5.8 enquire on what security mechanisms they have been usedin securing their data confidentiality from any kind of cyber-attacks. A major portion said they used anti-virus to secure their devices and data and they update their password frequently.Sreehari et al. (2018) also found that the major number of respondents installed anti-virus and update their passwords to secure themselves. On the contrary, a few numbers of the respondent open the email and talk with an unknown person online. The respondents fairly deleted social media app and account if they face any difficulties.

Conclusion

The current cyber-attack aptitude demands enhance attention for preventing cybercrime because prevention is always better than cure. With the flow of time internet using rate is increasing dramatically, the present study found 95% of respondents usesthe internet on a daily basis which is a surprising amount, and the possibilities of being victimized or accused by cybercrime are not so less. However Cybercrime is the latest form of crime so it is difficult to detect cybercrime, consequently, people need to learn all about cybercrime. Our research came to an illation that the ratio of awareness among the respondents regarding cybercrime is high for hacking when compare to others which are 61.4%.But having a good command of all types of cybercrime is beyond unavoidable. It is kind of obvious from the investigation that the respondents have limited knowledge about the procedure of ensuring data safety which is also a hazard. A few proposals have been put to this paper to enhance awarenessand strengthen cybersecurity in Bangladesh.

Implications

As the amount of cybercrime is increasing in our country, the following steps should be followed to make awareness about cybercrime among the internet user as well as the government.

1. It is recommended the internet users should use a firewall on their computers.
2. Intrusion detection software might be installed on the client computer so as to provide a warning to the user regarding any security breach.

3. Rules and regulations that deal with cyber-criminal should be strengthened so as to bring a sense of safety among internet users.
4. Educating the students about cybercrime and its impacts from the very beginning of the schools.
5. The college and universities should organize a workshop on cybercrime and cybersecurity.
6. Internet users should use a strong password and update their password at a regular interval.
7. It is suggested social media users should communicate only with the known person.
8. The government should arrangean awareness campaign about cybercrime.
9. The laws of cybercrime should be stronger and the guilty one should be punished according to the law as soon as possible.
10. Internet users must backup their valuable data to avoid data loss by cybercrime.
11. The internet users must strictly use antivirus software for their devices and update it on a regular basis.

References

Ahmed, S., Kabir, A., Sharmin, S., &Jafrin, S. (2017). Cyber-crimes Against Womenfolk on

Social Networks: Bangladesh Context. *International Journal of Computer Applications*, *174*(4), 9–15. https://doi.org/10.5120/ijca2017915407

Faisal, K. (2016). *Recent Trend and Issues of Cybercrimes in Bangladesh: An Analytical*

Study (Master's dissertation). Retrieved from 10.13140/RG.2.2.31917.33766

Kabir, N. (2018, March 31). Cyber Crime a New Form of Violence Against Women: From the

Case Study of Bangladesh by Natasha Kabir :: SSRN. Retrieved November 28, 2019, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3153467

Kumbhar, Dr. M., &Gavekar, Dr. V. (2017). A Study of Cyber Crime Awareness for Prevention

and its Impact. *International Journal of Recent Trends in Engineering and Research*, *3*(10), 240–246. https://doi.org/10.23883/ijrter.2017.3480.jtu50

Kundu, S., Islam, K. A., Jui, T. T., Rail, S., Hossain, Md. A., & Chowdhury, I. H. (2018). Cyber

crime trend in Bangladesh, an analysis and ways out to combat the threat. *2018 20th International Conference on Advanced Communication Technology (ICACT)*. https://doi.org/10.23919/icact.2018.8323800

Mostufa Kamal, M., Chowdhury, I. A., Haque, N., Chowdhury, M. I., & Islam, M. N. (2012a).

Natur of Cyber Crime and Its Impacts on Young People: A Case from Bangladesh. *Asian Social Science*, *8*(15), 171–175. https://doi.org/10.5539/ass.v8n15p171

Mia, B. (2015). Cybercrime and its Impact in Bangladesh: A Quest for Necessary

Legislation. *International Journal of Law and Legal Jurisprudence Studies*, *2*(4). Retrieved from https://www.academia.edu/13465468/

Shabnam, N., Omar Faruk, M., &Kamruzzaman, M. (2016). Underlying Causes of Cyber-

Criminality and Victimization: An Empirical Study on Students. *Social Sciences*, *5*(1), 1–6. https://doi.org/10.11648/j.ss.20160501.11

Sharmeen Karim, S. (2016). Cyber-crime Scenario in Banking Sector of Bangladesh: An

Overview. *The Cost & Management*, *44*(2), 13–15. Retrieved from http://www.icmab.org.bd/images/stories/journal/2016/Mar-Apr/3.Cyber-crime.pdf

Sarker, S.&R. Shahid, A. (2018). Cyberbullying of High School Students in Bangladesh:

An Exploratory Study. Retrieved from https://www.researchgate.net/publication/330132918

Sreehari, A., Abinanth, K. J., Sujith, B., Unnikuttan, P. S., &Jayashree, Mrs. (2018). A Study of

Awareness of Cyber Crime among College Students with Special Reference to Kochi. *International Journal of Pure and Applied Mathematics*, *119*(16), 1353–1358. Retrieved from http://www.acadpubl.eu/hub/

Sarwar, D. (2019, March 28). 3,659 cybercrime cases filled over 6 years, only 25

punished. *DhakaTribune*. Retrieved from https://www.dhakatribune.com/bangladesh/court/2019/03/28/3-659-cybercrime-cases-filled-over-6-years-only-25-punished