International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 01 | Jan 2023 www.irjet.net p-ISSN: 2395-0072

Cyber Crime: Youth in Social Decline

Md. Kabir Hossain[1], Mohammad Arif[2]

[1]Assistant Professor (ICT), Bandarban Cantonment Public School & College, Bandarban, Bangladesh.
[2]Student, 5th Batch, Dept. of Computer Science and Engineering, University of Creative Technology Chattogram

---

Abstract - *Information Technology (IT) is one of the priorities of the Bangladesh government. The country is quite advanced in this sector. New technologies such as mobiles and the Internet have spread beyond the city limits to the countryside. Various benefits of information technology are becoming increasingly available to people. Now anyone can easily communicate with anyone anywhere in the world. With the rapid expansion of information technology, cyber crime or IT-based crimes are also increasing rapidly. Innocent people are victims of various crimes. Again, various conspiracies are going on against the government using information technology facilities to perpetuate personal interests or party interests. Various rumors are being spread. Different groups are being provoked. Violent communalism is spreading as social crimes are happening.*

Key Words: ICT, Cyber crime, Cyberbullying, Social Media, Hackers, Extremists, Low enforcement agencies, ICT act, etc

1. Introduction

People from every sector in Bangladesh have poor or no concern about how their information is disseminated online and the protection of personal information which is why cyber-crime is growing rapidly in Bangladesh. The general public seems to have little interest in learning about this virus and has no idea how to protect themselves from it. Unfortunately, cyber criminals have used this to their advantage and are looking to exploit that fear and uncertainty for financial gain. Cyber criminals use phishing, smishing and fraudulent websites to extort personal information or gain access to an organisation's computer systems in search of valuable business and financial information. Emails and messages appear to be from an authentic source; In fact, fraudsters present themselves as genuine.

2. Conceptual overview of cybercrime

Cybercrime is apparently a 'crime' committed using 'computers' or 'networks' or 'hardware devices' or 'cyberspace'. The Council of Europe's Cybercrime Convention uses the term 'cybercrime' to refer to crimes ranging from criminal activity against data to content and copyright infringement. Cybercrime is generally defined as a crime in which a computer is used as a target or tool to commit a crime.

Cybercrime has many forms and new forms and techniques are being noticed day by day. However, the main forms of cyber crime are attached below:

Fig -1: Forms of Cybercrime

Cybercriminals are an ever-present threat in every country connected to the Internet. Cyber criminals consist of different groups or categories as shown below:

Fig -2: Forms of Cyber Criminals

3. Social media and its users

Every 3 seconds a social media ID is being opened on different platforms. According to the data of Bangladesh Telecommunication Regulatory Commission, the number of internet users in the country is about 112613000. And the number of mobile sim users is about 16000000. A large part of digital crime is being committed through social media through deception and enticement. Hacking social media accounts by compromising or creating fake accounts. Cyber-bullying is the use of insulting or defamatory comments directed at someone over the Internet or social media to humiliate them and undermine their social status by spreading unwanted content. Due to these reasons, the netizens are now facing various problems in using social media. Many are falling prey to cyber-criminals through Facebook, Messenger, Twitter, Viber, YouTube, WhatsApp and IMO etc. These virtual platforms exploit one's personal vulnerability to humiliate, intimidate or lure someone into doing something unfair. Teenagers are the first victims of such harassment. Adults or minors are constantly falling into this trap.

4. Cyberbullying

A large number of online social media users, including students of various educational institutions in Bangladesh, are victims of cyberbullying. According to data, 49 percent of school children in the country are victims of regular cyber bullying. According to the Ministry of Posts and Telecommunications, three-fourths of women in the country are victims of cyberbullying. However, this issue remains unaddressed. Only 28 percent reported harassment online. Others fear that they will be socially stigmatized if they complain. In addition to cyberbullying, this type of harassment is often happening on mobile phones, e-mails or mobile banking. As a result, depression, inattention to studies and insomnia etc. develop among the victims including women. Even suicides are happening. Children who are victims of cyberbullying are gradually turning to something terrible, the effects of which are devastating and almost irreversible. Below is a statistic showing the percentage of children who are victims of cyberbullying in some cases.

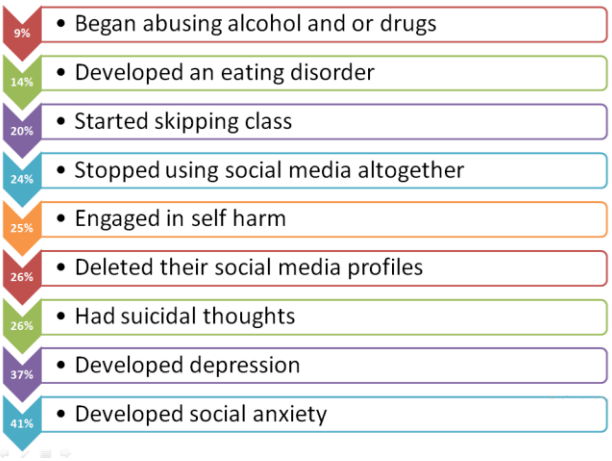

Fig -3: Effects of cyberbullying in kids

A survey has been conducted among people of different ages in our country and it has been found that they are the most victims of cyber bullying through social media. The rate of cyberbullying varies across different social media. Below is a survey of this:

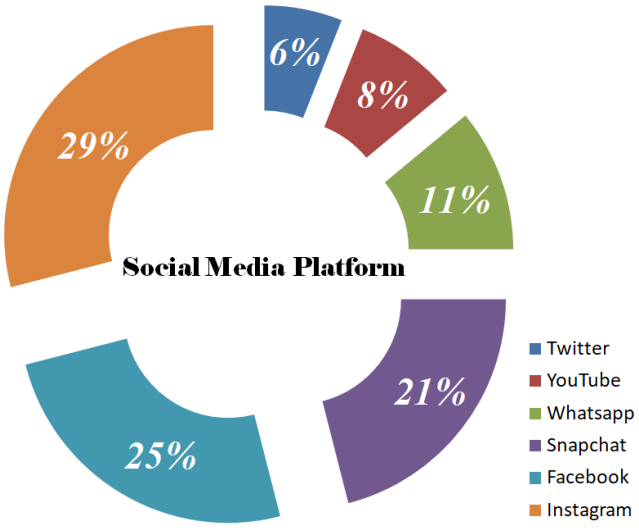

Fig -4: People are cyberbullied in different social media

5. Extremists and their activities

An organized clique is actively trying to mislead interested youth about the benefits of IT. Various religious extremist ideologies are being propagated by opening Facebook pages, groups, YouTube channels. Day by day, crores of people are joining it. Strict cyber monitoring should be done so that no one can disturb the security of the state. Internet access made easy. It has many advantages. There are also some downsides. So, when we do a good deed, the bad that comes with it will not cause a big crisis. Necessary steps should be taken for that. Therefore, if these cybercrimes continue, the security of the state will be under threat. It also poses a threat to public safety. The young generation is being

misled. Thus making life miserable for the youth and pushing them towards an uncertain future. Adequate measures should be taken by creating various units or organizations to monitor cybercrime in the interests of individuals and the state. As we have become digitally dependent, there is no substitute for cybercrime monitoring.

6. Digital platform and its weaknesses

Our government system is going digital. Hence, cyberspace threats will grow more alarmingly in the future. Social media including Facebook-YouTube should be strictly monitored. These cannot be solved simply by closing them and keeping users away. We are becoming dependent in some places, but enemies inside and outside the country have become quite active. They are ready to harm people in every possible way. How can it be prevented? Measures must be taken to protect us from any form of cyber-attack. Criminal gangs are becoming more reckless day by day as the existing laws of the country are weak in detecting IT-related crimes. This is undoubtedly terrifying. BTRC was seen helpless in this regard. This time during Durga Puja, there have been incidents of communal attacks in different parts of the country on charges of insulting religion. As a result, the question has arisen - whether popular services like Facebook, YouTube, Twitter and Google will remain unregulated in this country or not. The question arises again and again. According to the number of mobile phone users, Bangladesh ranks the 10th in the world. Currently, the number of mobile subscribers in the country is about 16 crores. As the number of internet users increases due to accessibility, so does the number of cyber crimes. Especially the number of crimes centered on the social media Facebook is increasing. In this age of technology, living without computers, internet and mobile phones is almost impossible. Technology has become human-oriented and has bound people in all directions. As much as it is true and in the reality of the age its abuse is also becoming one of the causes of human suffering. School-going young women are the main victims of these frauds. Not only cyber crimes are being committed to victimize women, cyber criminals are also committing heinous crimes financially. Hacking mobile phone numbers with fake messages and stealing money from bank accounts are common.

7. Invention of new technologies and new tricks of deception

Another major criminal trend is spreading state, social, political and religious hatred on the Internet. We often see news of Internet-centric fraud and crime in the news. But law enforcement officials say crime levels are high and many crimes go unreported. Many do not report to the police or any other agency for fear of losing their dignity. As a result, many cases do not go to trial and in many cases the culprits cannot be identified. In this case, experts are talking about our technological limitations. It should be noted that as cybercrime is on the rise, the criminal investigation force needs to be trained to combat it. New technologies are being invented almost every day and criminals are committing crimes using those technologies. There can be no substitute for developing a technological law enforcement force to detect and suppress cyber criminals in the interest of protecting the country's security and reputation. Besides, modern laws are needed. They have not yet developed in the country. Many countries around the world have enacted laws to regulate social media. We have to pay attention to that too.

8. Actions by law enforcement agencies to mitigate cyber crime

A policy of silence against cybercrime is one of the major causes of damage. Fearing loss of family or honor, many tolerate or repress in silence. As a result criminals take more chances. They also lure victims into various traps to get financial benefits. In this age of internet we all are more or less facing a complex psychological problem like cyber bullying. Offenders are specifically accusing or attacking a person in public. Harassment also involves defacing someone's photos or videos and posting them online It is a type of cybercrime. There are specific laws and enforcement in the country to curb these crimes like cyber bullying. Just need to be aware of it. If the matter goes beyond the family circle, the law should be resorted to. Avoiding the cooperation of the police in this case is rather dangerous. This difficult task becomes very easy by following few steps. The first step is to file a General Diary (GD) at the police station. Evidence of harassment must be accompanied by screenshots or messages. Anyone who has been harassed can now get help by calling 999 or the police Facebook page. Such issues can also be resolved confidentially on the Ministry of Women and Child Affairs hotline number 10921. Complaints can also be made directly to BTRC's phone and e-mail. In the online world, there are ways to find a solution.

9. Challenges in identifying cybercriminals

Identifying, arresting and proving the charges against cyber criminals is time consuming and challenging for cyber security and crime departments. These challenges include lack of Mutual Legal Assistance Treaty (MLAT) with various countries, negligence of Internet Service Providers in storing log data, failure to promptly report an organized crime and lack of awareness and skilled manpower among digital technology users.

Here some difficulties to investigate cybercrime by law enforcement agencies. These are shown below:

- Under ICTA 2006, the offenses are non-cognizable (Section-76(2)) and the police cannot be investigated without a warrant. This takes away the freedom of investigation from the law enforcement authorities.
- At present, apart from two specialized units under the CID, no other police agency is capable of handling

cybercrime issues and these units are severely lacking in trained investigators, equipment and manpower.

- Difficulty in defining crime, jurisdictional issues, detection techniques and collection of digital evidence are also complex areas in cyber crime investigation.
- There are no dedicated analytics sites compatible with global secure police communication systems to provide real-time monitoring of cyber activities.
- Digital Forensic Laboratory is essential for cyber crime investigation and detection with professional experts, which we have a serious shortage of.

Various teams are working on cybercrime such as Digital Forensic Investigation Team, Cyber Incident Response and Investigation, Internet Referral and Investigation, Social Media Monitoring, E-Fraud Investigation etc. From the forgoing discussion certain recommendations are appended below for due consideration:

- ✓ Formulate a National Cyber Security Policy as well as establish an entity for overall coordinating and directing responsibility. BTRC may be strengthened to develop as regulatory body of cyber related issues.
- ✓ Create appropriate structures at all level with well-defined role and responsibilities so that human resources with adequate skills, knowledge and training are available to securely manage the information infrastructure.
- ✓ Create awareness and build momentum. Conduct extensive media campaigns and other civic activities to build mass awareness on cyber criminal activities. Initiate programs to educate everybody about their cyber right and also edify parents on how to filter harmful Internet contents.
- ✓ Initiate dialogs with the NGOs, donor organizations and corporate bodies for sharing government's vision and tentative roadmap towards combating cybercrime.
- ✓ Encourage senior officials of government and government agencies to carefully learn the basic operations of the Internet in order to work independently.
- ✓ Enhance law enforcement capacity to prevent and prosecute cyber attacks.
- ✓ Enact strict laws to deal with the menace of cybercrime. Laws should create deterrence in the minds of criminals.
- ✓ Every effort should be made for international cooperation to enable information sharing, reduce vulnerabilities and deter malicious users.
- ✓ A national level organization may be created for sanitization of hardware, software and computer related gadgets specially used in sensitive institutions.

10. Conclusions

Our dependence on the network will only increase in the years ahead. As technology advances, threats and vulnerabilities change, and understanding of information security issues improves, there is a constant need to review cyber strategy. Those sharing videos or spreading messages of social unrest on Facebook, YouTube or social media are being identified. Besides, it has become necessary to find those involved behind the rumor or video and take legal action. Many local and foreign gangs are regularly looting large sums of money by fooling common people in the cyber world. Criminals are placing such apps in front of Bigo Live, TikTok. But there is a big financial crime behind it. Cyber crime cannot be eradicated from cyber space. It is quite possible to check them. History has witnessed that no law has completely eradicated crime from the world. The only possible course of action is to make people aware of their rights and duties and to make law enforcement more stringent in curbing crime. Computer and information security, data protection, and privacy are all growing issues. No single technology or product will eliminate threats and risks. Securing our computer, information and communications networks protects our economy and our nation. Finally, it can be presented that the combined efforts of the government and the people is a possible way to realize the people's dream of digital Bangladesh and protect the individual and national security of the state from the aggression of cybercriminals. These misinformation and propaganda on social media and online must be stopped now and people from all walks of life must come forward. Remember our new enemies are just a mouse click away.

REFERENCES

[1] https://ictd.gov.bd/
[2] http://www.bbs.gov.bd/
[3] https://www.thedailystar.net
[4] https://www.police.gov.bd
[5] https://www.cid.gov.bd/
[6] https://www.dosomething.org
[7] https://www.researchgate.net
[8] https://www.broadbandsearch.net
[9] https://www.youtube.com/