People Need to Forward Morally to Suppress Cyber Crime

Jasim Uddin[1], Md. Abubakar[2], Md. Moniruzzaman Tushar[3], Mohammad Haydar Ali Chowdury[4]

[1]*Instructor (Tech.), Dept. of AIDT, Chattogram Mohila Polytechnic Institute, Chattogram, Bangladesh*
[2]*Instructor (Tech.), Dept. of Civil, SRA Institute of Science and Technology, Dinajpur, Bangladesh*
[3]*Instructor (Tech.), Dept. of Textile, Chattogram Technical School & College, Chattogram, Bangladesh*
[4]*Instructor (Tech.), Dept. of Computer, Chattogram Mohila Polytechnic Institute, Chattogram, Bangladesh*

---***---

Abstract - *Cyber crime is defined as a crime that occurs using a network-connected device, such as a computer or mobile phone. Those who commit cyber-crimes are known as cyber criminals or cyber crooks. With increasing digitization, internet crime is also on the rise. For example, such crimes may occur from a distance; For example - in a foreign country, most criminals prefer this method because the risk of being found and punished is limited. The most common types of cybercrime are phishing, hacking, cyber bullying, identity theft and spamming. Let me explain what these terms mean. To prevent cyber crime, I must first use my basic intelligence to judge what I can be a victim of.*

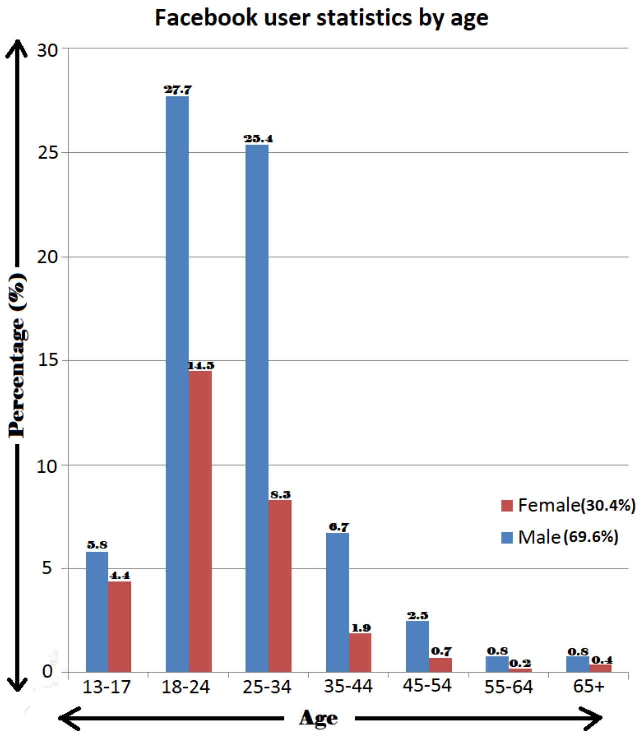
Key Words: *Cyber Crime*

1. Introduction

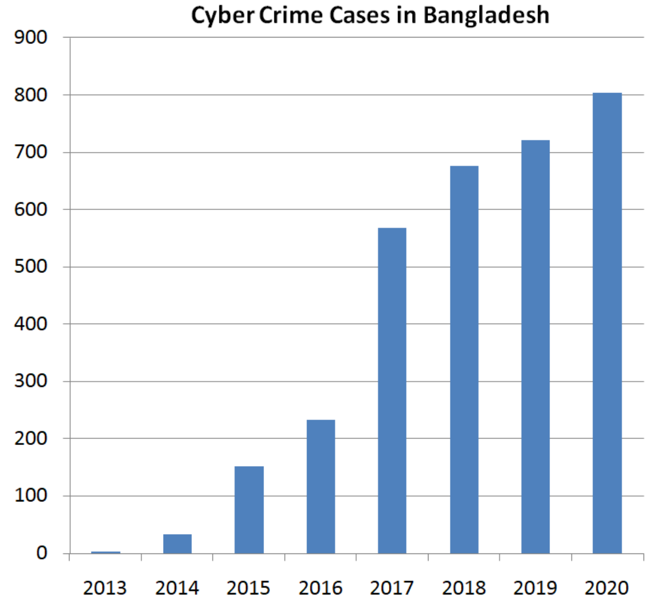
Information technology is at the top of the list of priorities of the present government in Bangladesh. The country is moving forward with a good reputation in this sector. New technologies, mobile and internet have spread beyond the city limits to the rural areas. The various benefits of information technology are becoming increasingly available to people. Communicating with people anywhere in the world is no longer a complicated matter for anyone. With the rapid expansion of information technology, cyber crime or information technology based crime is also increasing rapidly. Innocent people are being victims of various crimes. Again, various conspiracies are going on against the government using the benefits of information technology. Various rumours are being spread. Different groups are being provoked. Violent communalism is spreading as social crime is happening.

2. Social Media and Current Context

Every 12 seconds a social media ID is opened in our country Bangladesh on various platforms like Facebook, Twitter, WhatsApp, Instagram, Telegram. According to the BTRC data, now the number of Internet users in the country is 11 crore 26 lakh 13 thousand. And the number of mobile SIM users is not less. That is about 16 crore. According to the data available in October 2020, the number of Facebook users in Bangladesh is 43360000 which are 25.3% of the total population. The number of men is more. Males and females are 69.8% and 30.4% respectively.



A large part of the crimes committed through digital are now through social media. Hacking social media accounts is called compromising. Or create a fake account. There are also crimes like cyber bullying and misleading people by spreading unwanted content. Netizens are now facing various problems on social media. Many are falling prey to cyber criminals through Facebook, Messenger, Twitter, Viber, YouTube, WhatsApp, Emo, etc. These virtual platforms exploit someone's personal weaknesses to humiliate, intimidate or tempt them to do something unjust. Adolescents were the first victims of such harassment. Young children and adolescents are the first victims of such harassment. Now boys and girls of different ages are constantly falling into this trap.

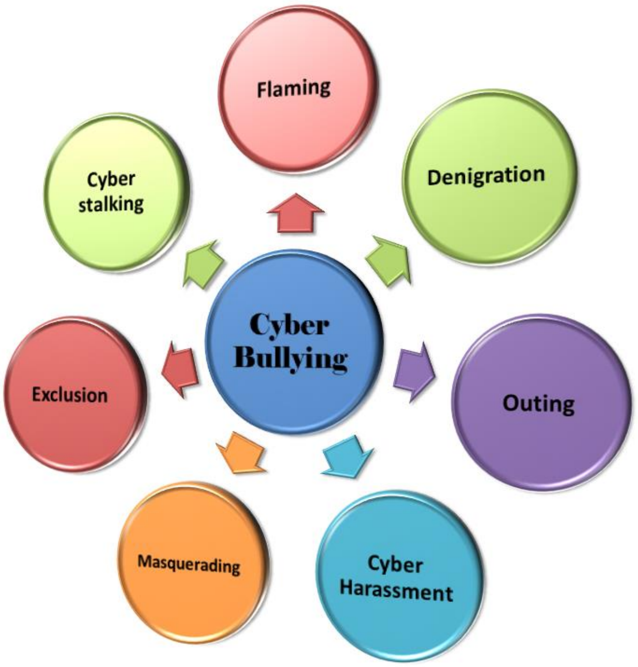


In Bangladesh, a large number of Facebook users, including school, college and university students, are victims of cyber bullying. According to the data, 49 percent of school children in the country are regular victims of cyber bullying. According to the Ministry of Posts and Telecommunications, three-quarters of the country's women are victims of cyber bullying. However, this issue remains unpublished. Only 26 percent complained of online harassment. Others are afraid that if they complain, they will be socially degraded. Apart from cyber bullying, such harassment is also happening on mobile phones or e-mails. As a result, there is a lot of frustration among the victims including women, inattention to studies, insomnia etc. Even suicides do happen.

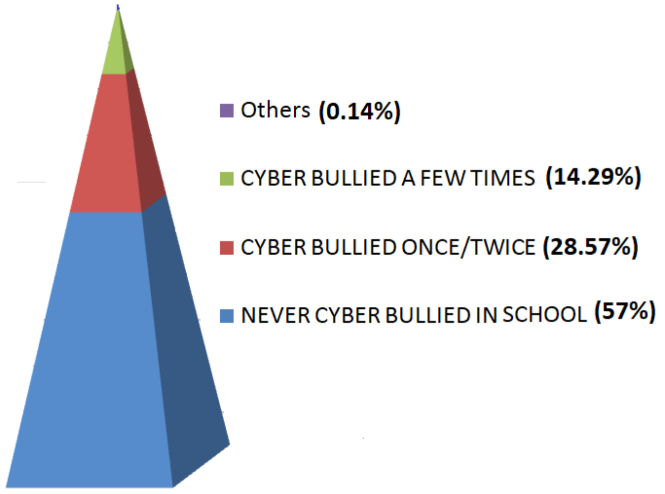
The following are the common online victims of cyber bullying:

- Social Media, such as Facebook, Instagram, Snapchat, and Tik Tok
- Text messaging and messaging apps on mobile or tablet devices
- Instant messaging, direct messaging, and online chatting over the internet
- Online forums, chat rooms, and message boards, such as Reddit
- Email
- Online gaming communities

Victims are usually the victims of various forms of cyber bullying. Different types of cyber bullying are shown below through radial chart.

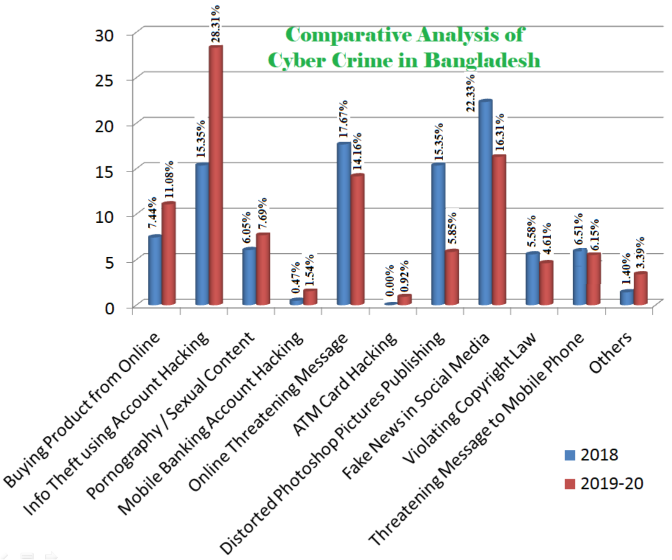


The number of students who have been the victim of cyber bullying once / twice is 27.56%. The number of students who have been the victim of cyber bullying a few times is 14.29% and the number of students who have not been the victim of cyber bullying at school by someone is 56%. Another study on cyber bullying found that more than 32% of boys are prone to cyber bullying. 27.3% of sufferers suffer from various mental illnesses. 9.1% of sufferers have a condition called depression. 60.87% of bullies maintain relationships with victims as virtual friends. Here shows the statistics of cyber bullying among school-going children in Bangladesh.

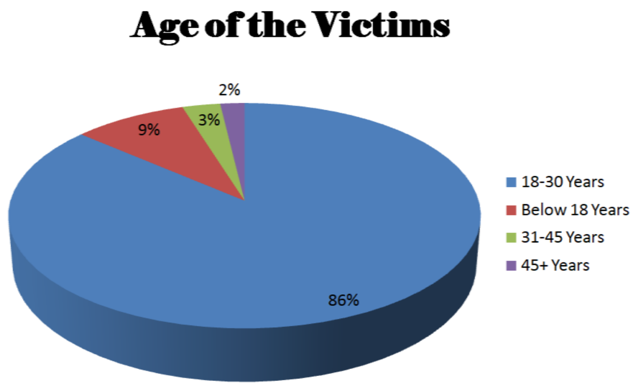


3. Comparative Analysis of Cyber Crime

Based on the results of various surveys in the light of the information provided by the victims, it has been found that the crimes that are organized through the phone calls of the crime cycle cover 6.51% of all the crimes. Crimes are organized at a rate of 5.58% through copyright infringement. Criminals carry out their premeditated crime by promising jobs at 1.40% and selling fraudulent products at 0.47%. These are all fancy forms of crime. According to the CCA Foundation's (Cyber Crime Awareness Foundation) 2018 research report, there has been a significant increase in pornography-related crimes (2.25% to 6.05%). On the other hand, despite the decline from 27.07% to 22.33%, many Internet users have been the victims of misinformation. Manipulation through intentional distortion and image editing remains the same as in 2018 at 15.35%. However, the percentage of victims in e-commerce and online banking process decreased from 8.27% to 7.44%. Comparison of cyber crime statistics: Survey of victims at individual level shows that cyber crime has increased alarmingly in the country in 2019-2020. Online account hacking or information theft including social media has also increased alarmingly that was not observed before. The corona virus situation has led to an increase in online shopping and more people than ever before have been deceived into buying products online. This year's survey analyses the comparative statistics of cyber crime and shows that the incidence of social media account hacking is in the first place with a rate of 26.31%. Based on the report of 2019, this rate was 15.35% which is about 13% less than this time. Although in the report of 2019, the incidence of propaganda through social media was 22.33%, but this time the number has come down to 18.31%.



During the survey, we found that most people between the ages of 18 and 30 are victims of cyber crime, accounting for 86.9% of the total victims. The second highest number of victims was under 18 years of age and accounted for 8.93% of the total victims.



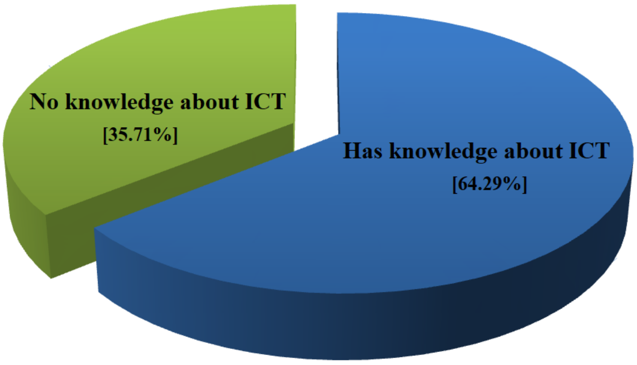
4. Cyber Crime Monitoring Facilities

An organized group is actively trying to confuse the passionate soft hearted youth with the benefits of information technology. These extremist ideological circles are taking advantage of the internet by opening Facebook pages, groups and YouTube channels to spread various religious extremist ideologies. As the days go by, billions of people are joining it and including themselves in their group. Parents are losing control of their children. This requires strict cyber monitoring so that no one can disrupt the security of the state. Internet facility has become easy. It has many good aspects. There are also some bad aspects. So when you do a good deed, the bad that comes with it should not cause a big crisis. For this, necessary and epoch-making steps have to be taken. So cyber crime is now a threat to the security of the state. It also threats to public safety. The young generation is being misled. The lives of young people are being made miserable by these various online based activities. It is important to take adequate measures to monitor cyber crime. As we become digitally dependent, there is no alternative to cyber crime monitoring. Our state system is going digital, so the threat of cyberspace will increase even more terribly in the future. Social media including Facebook-YouTube should be strictly monitored. It is not possible to stay away by closing them again. We are becoming dependent in some places, we have to make arrangements to prevent any kind of attack by the enemy inside and outside the country, how to prevent it, so that we can be protected from any kind of cyber attack.

5. Revised Conventional Law to Suppress ICT Crime

The criminal gangs are becoming reckless day by day thinking that the existing laws of the country are weak in identifying information technology crimes. The matter is undoubtedly terrifying. The Bangladesh Telecommunication Regulatory Commission (BTRC) has been seen to be helpless in this regard. At different times, there have been incidents of communal attacks in different parts of the country accusing the followers of minority religions of insulting religion at religious festivals. As a result, the question has arisen - whether popular services like Facebook, YouTube, Twitter and Google will remain uncontrolled in this country -

the question is coming up again and again. Bangladesh ranks tenth in the world in terms of number of mobile subscribers. At present the number of mobile subscribers in Bangladesh is about 16 crore. As the number of internet users is increasing on the one hand due to easy availability, so is cyber crime on the other hand. In particular, most of the crimes organized by social media are shown on Facebook platform. In this age of technology living without computer, internet, mobile phone is almost impossible. People of all walks of life have become technology oriented today and again this technology has bound people around. As true as it is and the reality of the age, its misuse is also becoming one of the causes of human suffering. Young school-college girls are the main victims of these scams. Not only is cyber crime being perpetrated for the purpose of abusing women, but cyber criminals are also committing heinous crimes financially. Hacking numbers with fake messages on mobile phones is a frequent occurrence and this method is considered to be the easiest way for criminals on mobile phones and stealing money from bank accounts.



Analysing the data, we found that 64.29% of the total victims knew ICT related laws and regulations. 35.71% on the other hand had no idea. Compared to the 2020 report, the number of victims with knowledge of ICT laws and regulations has increased by 27.29% this year. Last year, the percentage of educated group was only 37%, the other group was 63%.

6. Limitations on the use of Modern Technology

In addition, another major crime is the spread of state, social, political and religious hatred on the Internet. We often see news of internet centric fraud and crime in the media. However, law enforcement officials say that the level of crime is higher and many crimes are not reported in the media. Many people are not complaining to the police or any other organization for fear of losing their dignity. As a result, many cases are not brought to justice, and in many cases the culprits are not identified. Experts are talking about our technical limitations in this case. Keep in mind that as cyber crime grows so does the need to train crime investigators. Almost every day new technologies are being invented and criminals are using that technology to commit crimes. In the interest of protecting the security and reputation of the country, there can be no alternative but to build a technological law enforcement force to identify and suppress cyber criminals. Besides, up-to-date laws are required. They have not been developed in the country yet. Many countries in the world have legislated in this regard and brought social media under the law. We also need to pay attention to that.

7. Confidence and Courage in Law Enforcement

The policy of remaining silent in cyber crime is one of the reasons for the big loss. Many people endure or suppress all 'quietness' for fear of losing family or respect. Criminals take more chances as a result. They also trap the victim in various traps in order to get financial benefits. Cyber-attacks have become a complex psychological problem as everyone around the world has begun to enjoy the benefits of using the Internet everywhere. It has become commonplace to publicly accuse or attack someone with bad language. Bullying also involves distorting a person's picture or video and posting it online. It is a kind of cyber crime. However, there are laws in the country to suppress these crimes. Just need to be aware. If the matter goes beyond family boundaries, we have to take refuge in the law. In this case, it is better to avoid police cooperation. This difficult task can be easily remedied by following a few steps. The first of these is to make a GD at the police station. Evidence of harassment must be kept with. Screen shot or message. Anyone who is a victim of harassment can now get help by knocking on 999 or the police Facebook page. Victims also report their problems on the hotline number 10921 of the Ministry of Women and Children's Affairs on condition of anonymity. Those who are being harassed on phone and online will also be able to lodge complaints directly on BTRC phone and e-mail. If you are facing any kind of embarrassing situation in the online world, you can find a quick solution through these organizations. From the data we have collected, it can be deduced that out of 168 victims, only 36 sought help from law enforcement agencies, which are only 21.43%. Out of these 36 complaints, only 22.22% complaints have been resolved by the agencies. However, 72.22% of victims felt that the action taken against them was inadequate.

8. Challenges of Cyber Security and Crime Department

Identifying, arresting and proving allegations of cyber criminals is time consuming and challenging for the Department of Cyber Security and Crime. These challenges include lack of Mutual Legal Assistance Agreements (MLATs) with various countries, lack of Interpol assistance, lack of criminal exchange policy, indifference of Internet service providers to preserve user data logs, failure to report crimes in a timely manner and awareness among digital technology users and lack of skilled manpower. Digital Forensic Investigation Team, Cyber Incident Response and

Investigation, Internet Referral and Investigation, Social Media Monitoring, E-Fraud Investigation are working tirelessly on various types of cyber crimes.

9. Advice to the Stakeholders based on the Assessments

People need self-defense to protect them from cyber crime. In this context, based on our observations to the government and other stakeholders in ensuring crime control and cyber security, some suggestions are mentioned:

- ✓ Independent "Cyber Squad" formation
- ✓ Spreading awareness: Awareness can be broadcasted by
    - Mass Media
    - Educational Institutions
    - Initiatives by Government and private institutes
- ✓ Accessibility of legal help
- ✓ Increase efficient personnel in law enforcement agencies and gain the trust of people
- ✓ Proper utilization of political members
- ✓ E-commerce policy & controlling authority formation
- ✓ Remedy of porn addiction
- ✓ Cyber Security ensured for women and children
- ✓ Building efficient staffing in the cyber Security sector

10. Conclusion

Those who are sharing videos or spreading messages of social unrest through Facebook, YouTube or social media are being identified. Besides, it is becoming urgent to take legal action by finding out the people behind these rumors or videos. In the cyber world, by fooling the common people, many domestic and foreign circles are regularly looting large sums of money. Criminals are involved in a major financial crime using such apps as Bigo Live, TikTok. These abuses and propaganda on social media and online must be stopped now and people from all walks of life must come forward.

REFERENCES

[1] https://www.nature.com/articles/s41599-020-0430-7

[2] https://bangladeshpost.net/posts/cyber-research-report-2020-39393

[3] https://ccabd.org/

[4] https://www.reveantivirus.com/en/computer-security-threats/cybercrime

[5] https://www.ncbi.nlm.nih.gov

[6] https://www.digit.in

[7] https://www.pandasecurity.com