Bangladesh Cyber Research Report 2020

Zahin Yasar Reshad

As the number of internet users rises in the country, cybercrimes continue to increase at an alarming rate.The crimes that are prevalent in our society - violence, rumors, political propaganda, fake news, gang culture, suicide, pornography, cyber bullying, extortion, piracy - all have translated to digital platforms.

According to statistics published by the Bangladesh Tele Regulatory Commission (BTRC), the total number of internet users in July 2019 was 96 million 176 thousand, of which 94 million are mobile phone users. According to https://www.napoleoncat.com, the total number of Facebook users in Bangladesh in January 2019 was 33 million 713 thousand.

From farmers to professors, people of all classes have entered this virtual realm of networking – the internet. However, despite the large number of users, most people remain unaware about therisks associated with internet usage. And as a result, many fall victims of cybercrimes.

Today, the internet has become an integral part of our daily lives. Social welfare, economic development, and even national security are regulated via the internet. Under such circumstances, there is no alternative to raising mass awareness about individual accountability and controlled use of technology, data protection, and cyber security.

Research Objective

The main objective of this research is to identify the cybercrime victims, and come up with the means of helping them. And to reach this objective, several methods may be implemented:

- Identifying the type of cybercrimes to the individual level
- Informing users about the types of cybercrimes
- Determining the factors restricting victims from attaining legal aid
- Coming up with specific procedures for tackling cybercrime
- Regulating cybercrimes by overcoming the prevailing challenges

Research Methodology and Types

The Hourglass Methodology was practiced in this research. The research report was conducted through Q&A's with victims to the individual level and extensive reviewing and expert analysis of their comments. In this process, each of 134 victims was asked 18 questions, with the questions including:

- what forms of crime they have been victims of
- whether they've sought legal help
- reasons behind no legal actions, if any
- their experience after reporting the crime
- what they think is necessary as a remedy

Analysis structure

The results of the study have been analyzed based on some indicators that match with the objectives of the study. The following have been used as indicators in the survey:

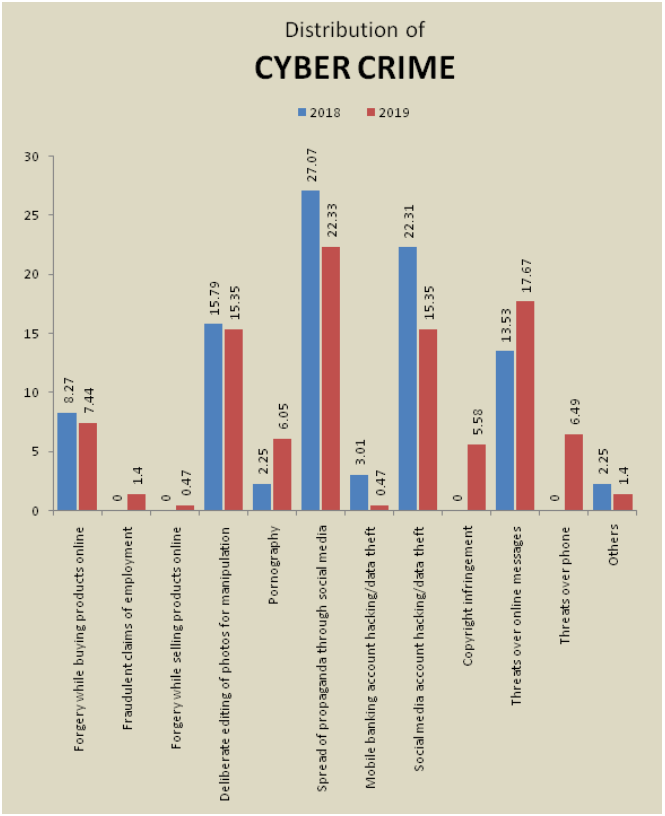
- type of crime
- seeking of legal aid
- satisfaction/dissatisfaction after filing complaint
- advice on cybercrime regulation by victims

Results

Today, crimes in the cyber world can be classified into eleven distinctions, of which four are novel. With time, new forms of crimes are emerging, as more people are falling victims of cyber misdemeanor. Amongst the victims, the proportion of females has risen to 16.77 percent. However, at 80.6% of the time, victims refrain from seeking legal aid after being affected.

Type of Crime

Upon surveying victims, we have discovered that the major form of cybercrime has been threats over phone calls, covering 6.51% of all crimes. Next is copyright infringement at 5.58%, fraudulent promises of employment at 1.40%, and fraudulent product sales at 0.47%. All these are novel forms



of offense.

According to the 2018 research report by CCA Foundation, there has been a significant rise in crimes related to pornography (2.25% to 6.05%).

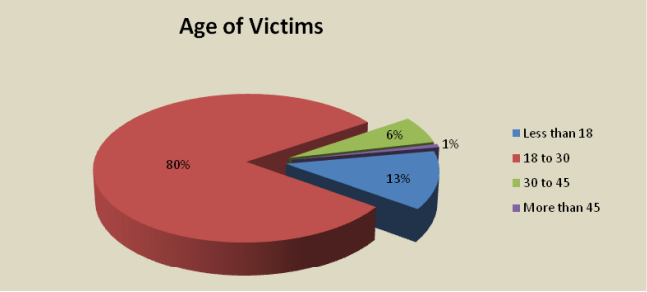
On the other hand, many internet users have been subjected to the spread of misinformation despite a decline in percentage from 27.07% to 22.33%.

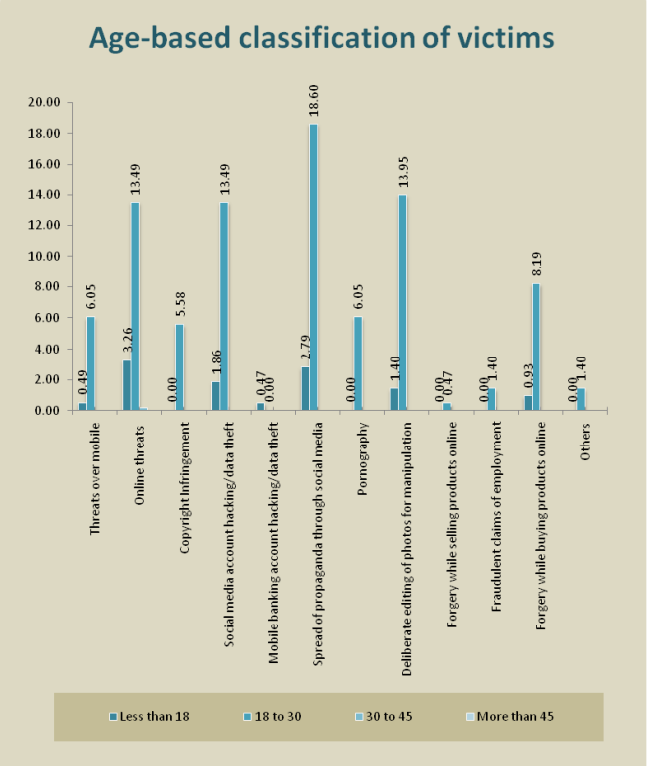
Manipulation through deliberate distortion and editing of images remains the same as in 2018, at 15.35%.

However, the percentage of people victimized in the process of e-commerce and online banking has declined from 8.27% to 7.44% and 3.0.

Age Classification of Victims

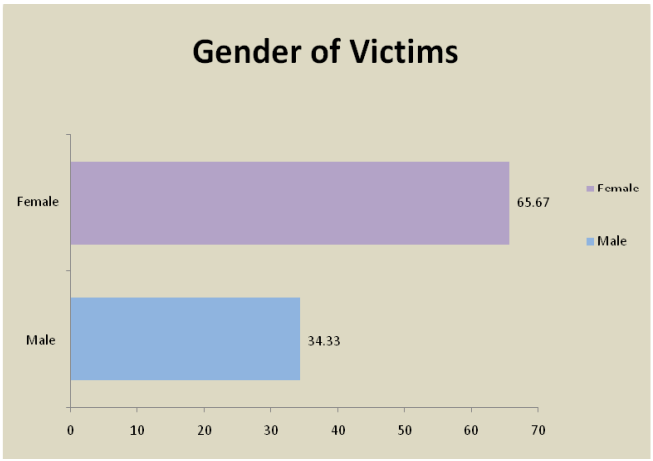
According to the survey, the modal class of victims is aged 18-30. Next are people aged below 18 at 11.16%, 30-45-year-olds at 3.72%, and people above 45 at 0.47%.





Gender Classification of Victims

This year, the percentage of females falling victims of the various forms of cybercrime has increased drastically from 51.13% to 67.90%. More so, of the people misled to believing false information in social media, 16.3% were women, while the remaining 6.05% were men. The tilt is also consistent for online threats; men comprise of 3.72% while women hold a staggering 14%.

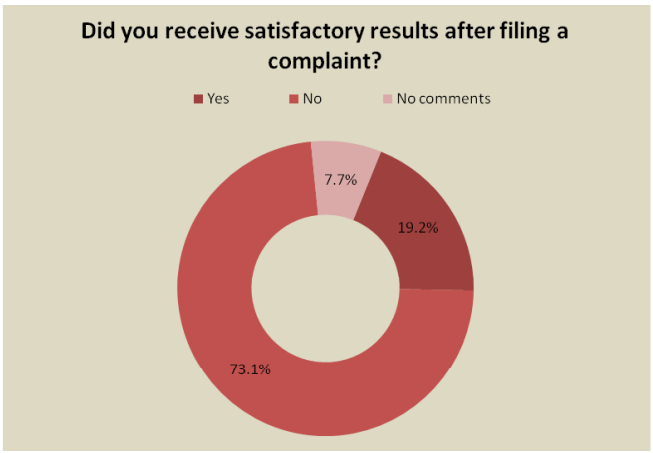


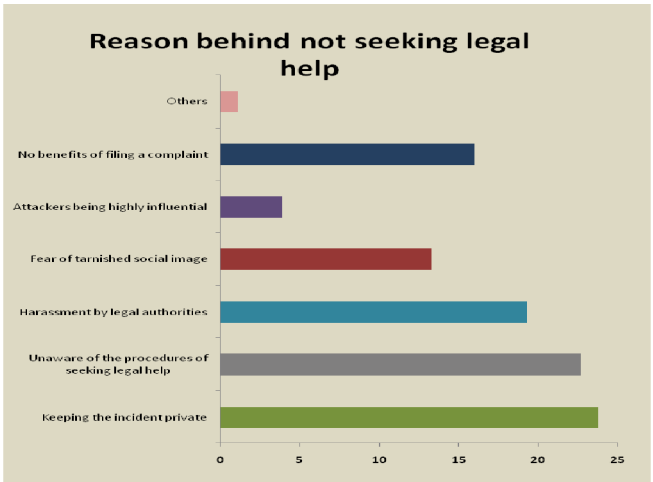
Seeking Legal Help

Although the government has enacted several digital security laws, victims seem to refrain from legal help. Only 19.4% of the people report these crimes, and a bare 19.2% receive satisfactory resultsafter complaining.

One of the reasons behind abstaining from legal aid is the preference of keeping the incident private. Such is prevalent at 23% of the cases. 22.7% of the people are unaware of the procedures of seeking legal help, and 19.3% fear being harassed by legal authorities.

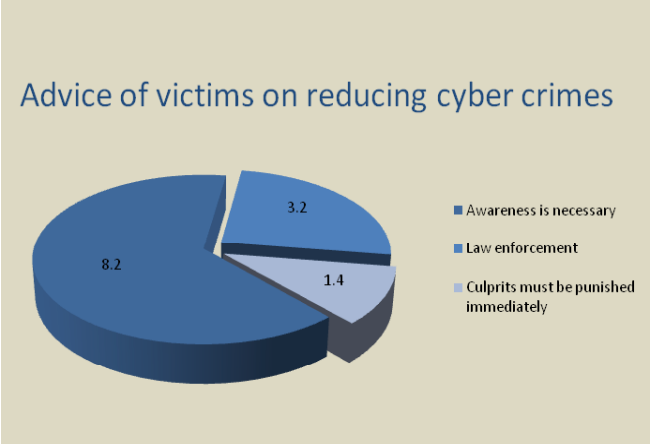
Moreover, 13.3% of the victims fear tarnishing their social image, and 3.9%avoid legal helpthinking that the attackers are highly influential. On the other hand, 63% are unaware of the laws for protection against cybercrime.





Advice of the Victims

Compared to previous surveys, 34% of the victims feel that the situation would decline without spreading awareness about cybercrime. 20.1% feel that law enforcement is vital to counter the issues, and the remaining 45.9% agree that culprits should be punished immediately to obtain optimistic results.



Recommendations to improve the current conditions

Digital Bangladesh is now a reality: a reality that exposes us to the rest of the world and makes us global citizens. Consequently, it is vital to ensure that the safety of users is of the highest standard. The realm of the internet is similar to a castle of glass - exhibiting superior magnificence and versatility. At the same time, this implies that users will be prone to attacks in the form of cyber-attacks. To ensure a safe browsing experience, users must remain informed about the type and potency of these attacks. And to ensure this, the government and associated organizations must come forward and take necessary measures.

Activities to raise awareness

Awareness is the most effective means of countering cybercrime. Home routers must be kept under surveillance to track the navigation history of underage users in the house. And the guardians must conduct this inspection.

Since the young generation comprises the majority of internet users of the country, it is crucial to raise awareness amongst people in this age group. To do so, the government can choose to declare October as Cyber Awareness Month (CAM) as a part of international awareness campaigns.

While we can avail the services of law enforcement systems for crimes in the outside world, such facilities are unavailable in the cyber-world. Hence safety while surfing through the net becomes a personal responsibility. According to the CCA Foundation, at least 50% of the crimes committed in this virtual realm can be avoided just by raising awareness. And we can turn to the public as well as private companies for this. Initiatives may include broadcasting expert advice on the use of technology through posts, posters, flyers etc.

Law

The general public must receive cognition on the digital safety laws. According to data obtained from the research, 63% of all internet users are unaware of the bare existence of these laws. Hence, acknowledgment of these laws becomes a necessity.

Social Media

The biggest platform for raising awareness is undoubtedly social media. 'Crime and Cyber Awareness' can be highlighted in frequently regulated workshops on professional expertise development. Social media will be the most effective means of reaching people and ultimately raising awareness.

Safe Cyber Culture

The external world is changing now and then. To adapt to these changes and enjoy a safe internet experience, we need to learn about the constantly evolving threats of the cyber world. Attaining this will require initiatives by the government and associated cyber security firms. Schools, universities, and public and private sector firms should regularly organize workshops and seminars to encourage internet users to adhere to a safe cyber culture.

Including Cyber Security in Educational Curriculum

The introduction of cyber security to the educational curriculum will automatically seed the importance of cyber awareness into the next generational users. Making cyber awareness courses compulsory in primary and secondary schools will be a formidable step towards creating a safe internet.

Employing responsible and ethical candidates in tech-related posts

One of the grave issues of our country is corruption. The problem of cybercrimes gets aggravated if tech-based posts are occupied by unethical employees. At the same time, to ensure a safe networking environment in workplaces, firms should form cyber security policies that all employees must follow.

Forming a skilled workforce

Both governmental and non-governmental firms need to come forward to create international standard training centers throughout the country. An example of such a positive initiative is the introduction of Cyber Gym in the Military Institute of Science and Technology. Further improvements would include the establishment of quality research facilities to come up with solutions to cybercrimes.

Including skilled personnel in law enforcement posts

According to data accumulated from the research, 80.8% of all victims were dissatisfied with the help of law enforcement services after filing complaints. And this can be credited to the lack of expertise of personnel in law enforcement posts. Moreover, the evolving status of criminals in the cyber world further makes it compulsory for law enforcement officers in cyber wings to be highly skilled and efficient in the field.

Involvement of people in this field

Cyber security is a massive field. The sole involvement of the government will not be sufficient to build up a strong

cyber security structure; instead, the engagement of people working in this field will strengthen the national cyber security structure.

Prioritizing and popularizing local technology for social media

Information and technology influences much of our lifestyle. Our personal information acts as the fuel for technology. While this information can be used for both positive and negative purposes, encouragement of local technological forms as social media will help restrict the cynical use of personal data. To do so, local firms must also ensure a well-designed high-quality service.

Utilizing Immigrant Manpower

There are large numbers of patriots throughout the world with a thorough technological aptitude. These people may be enthusiastic about working with the government and other organizations to strengthen the cyber security structure of the country. One of the benefits of the cyber world is that people can work without being present at an office. Hence employing highly skilled people located in any part of the world is not impossible.

Government Patronage

While the government must host campaigns and workshops promoting cyber awareness, it should also encourage non-governmental and private organizations to raise awareness on their own. Governmental support will undoubtedly act as a boost for such private initiatives of raising awareness.i

Conclusion

The cyber-world is one of the greatest achievements of humans. The internet has brought the entire world to our grasp. We can now communicate with someone sitting on the other end of the planet: credits to the internet. However, the myriad opportunities have also exposed us to different and novel forms of cyber-attacks. Hence, we should remain careful while using the internet, and also inform others about the potential threats of this technology. As far as the implementation of cyber security laws are concerned, it remains a responsibility of social media workers, law enforcement services, tech assistance providers, lawyers, and even judges. Only then will we advance towards a safer networking experience CJ

Feedback: zahinyasar2001@gmail.com