www.ccabd.org

Cyber Crime Awareness Foundation

সাইবার ক্রাইম অ্যাওয়ারনেস ফাউন্ডেশন

Research Report

on

Cyber Crime Trends in Bangladesh-2021

Release Date: 18th June 2021, Dhaka

Cyber Crime Trends in Bangladesh-2021

Research Team

Monira Nazmi Jahan

Convener, Research Cell, CCA Foundation

Senior Lecturer, Dept. of Law, East West University

Research Associates:

Ariful Amir

Adhora Ema Barua

Khan Mohammad Abu Saleh

Md. Meshkat A Rabbani Shrestha

Sifatunnessa Hoque -

Research Assistant, East West University Chapter

Supervised By:

Kazi Mustafiz

President, Executive Committee, CCA Foundation

(Editor, cyberbarta.com)

Nurun Ashrafi

General Secretary

(Chairman, Media Mix Communications)

Tanziah Khanam

Training & Research Secretary

(Computer Software Engineer)

Md. Shahidullah

Office Secretary

(CEO, Color Express)

S M Imdadul Haque

Vice President

(Executive Editor, digibangla.tech)

Md. Zahidul Islam

Organizing Secretary

(CEO, Jadukor IT)

Abdur Rob

Finance Secretary

(Manager, Hajj & Omrah, Hasem Air International)

Research review and gratitude:

At different stages of collecting information, we are sincerely grateful to honourable advisors, other members of the Cyber Crime Awareness Foundation and well-wishers who have enriched the report with opinions, suggestions and cooperation.

Contact Us

Cyber Crime Awareness Foundation
ccabd.org
CSR Initiative of Cyber Paradise Ltd.

CYBER CRIME AWARENESS FOUNDATION (CCA FOUNDATION)

5/2 Lalmatia, Block: A, Flat: A4 (2nd floor), Mohammadpur, Dhaka 1207, Bangladesh.

+8801957616263 info@ccabd.org, aidcca@gmail.com www.ccabd.org

Cyber Crime Trends in Bangladesh-2021

1. Background

The whole world has fallen victim to Coronavirus and came to a standstill. Amidst the pandemic, everyone is trying to adjust to the new normal by doing their chores remotely or in-person while socially distancing themselves, and Bangladesh is no exception. To ensure safety of the masses, this densely populated country is forced into a lockdown. Nevertheless, thanks to the internet, over 11.5-crore people are now connected and participate in day-to-day financial activities and work. The internet is acting as a highway here, connecting everything, including health, education and entertainment. However, like an actual one, this highway is also prone to accidents. People knowingly and often unknowingly causing to and being victims of such accidents. They involve themselves in cybercrime without even realising, and the numbers are piling up with each passing day.

Slowly, this somewhat mandated use of the internet is turning into an addiction. Things have escalated so far that a teenager of 14 in Chandpur committed suicide because he could not manage to buy an internet pack to play games on his phone. This obnoxious attraction turned addiction is comparable to substance abuse. The only difference is that this addiction is purely behavioral, where substance abuse is merely chemical addiction.

According to the regulatory body, Bangladesh Teleregulatory Commission (BTRC), Bangladesh has 11.61 crores active internet users as of March 2021, and among them, almost 10.63-crore users are accessing the internet through their smartphones. Also, the number of Facebook users rose to 3.79 crores, according to NapoleonCat.

Even though the growing number of internet users is a good sign for a developing country like Bangladesh, it does not come without its own set of challenges. So much so that it has become a national concern, and to address this, there is no alternative to creating awareness about the cybercrime laws and safe internet.

To address the concern and ensure safe internet for everyone, Cyber Crime Awareness Foundation (CCA Foundation) is working tirelessly, and this report is a part of that initiative. CCA Foundation has identified some key points relating to cybercrime with the data acquired in surveys, further analysis and research while also working on a to-do plan for the future.

2. Goals

The goal of the "Digital Bangladesh" project was to ensure the availability of the internet to the farthest corners so that people from all aspects of life can take full advantage of the information, technology and internet.

This research aims to determine the current state of cybercrimes, their victims, and how we can prevent said crimes. The specifics are as follows:

2.1. To identify the types and nature of cybercrime

2.2. To pinpoint the nature of the crimes varying on age, profession and gender

2.3. To understand the crimes at a personal level

2.4. To determine the challenges of bringing victims to seek help from the law

2.5 To draw the attention of the relevant stakeholders and help them implement the rules and regulations.

3. Research Model & Structure

This research follows the hourglass model. Over the last two years, Cyber Crime Awareness Foundation has talked with victims of cybercrime and researched the subjects. To ensure the privacy of the victims, their names and identification are omitted from the report.

During the research, 168 victims were asked the same 18 questions along with their opinion on how to tackle the problem. They were also asked about the experience and questions like how they became victims of such crimes, what they did after the occurrence, and whether they asked the authorities for help – If not, why, etc.

4. Analysis Model

The results were analysed based on some indicators that comply with the motive of this research. A comparative analysis was done from the acquired data to see whether the victims went to the authorities after the occurrence, did they get satisfactory service from the authorities, etc. The data was also used to see whether the crimes vary on age and profession.

5. Results

The research report consists of 11 separate tabs.

Here we found out about the decrease in 4 specific types of cybercrime where 6 outgrew their previous records, leading to the emergence of a brand-new dimension of cybercrime. Overall, the number of such crimes is increasing, and the rate of complaints to authorities so far has been disappointing, which indicates the crying need for cyber literacy among the masses.

5.1 Types of Crime

During the 2019-2020 period, cybercrimes relating to social account hacking and identity theft increased at an alarming rate. The survey also found that ATM card hacking is at its best in the pandemic as people relied heavily on online shopping, leading to unflattering encounters with malicious circles that are after victim's card information.

From the survey, we also found that the most common type of cybercrime in 2020 was social media and other personal account hacking, which totalled 28.31%, while in 2019, it was merely 15.35%. This means hacking and theft of personal accounts increased almost 13% from 2019 to 2020.

Contrasting that, we found a steady decline in the spread of misinformation or fake news. The rate fell from 22.33% in 2019 to 16.31% in 2020. However, sexual harassment and revenge porn cases have increased to 7.69% from 6.05% in 2019.

Despite the increase in sexual harassment cases, the sigh of relief is the decrease of cases with photo manipulation, which came down to 5.85% in 2020, less than half of what we surveyed in 2019.

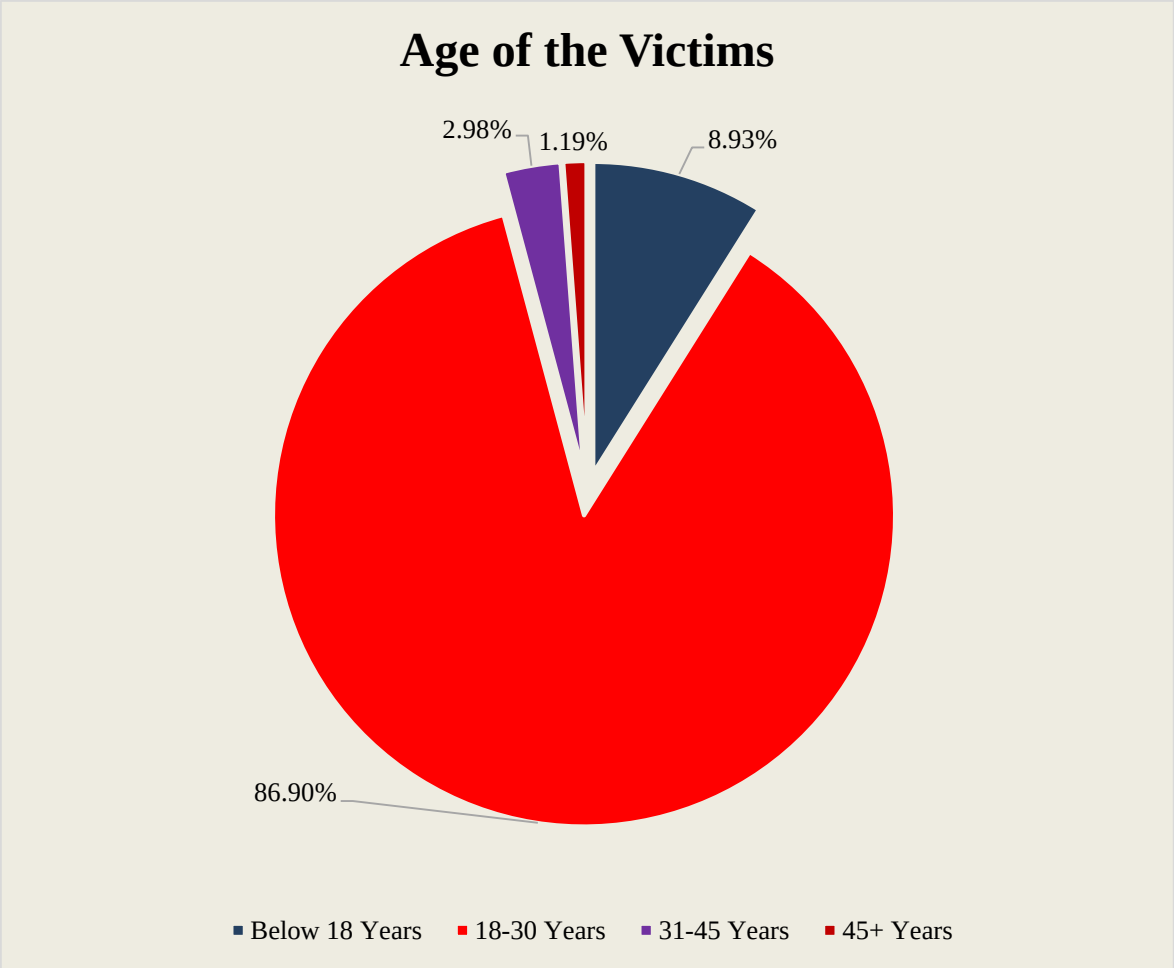
Another cyber offence that has taken a fall is text threats made with phones. The crime rate came down to 14.16%, which is almost 3% less than the previous year's 17.67%.

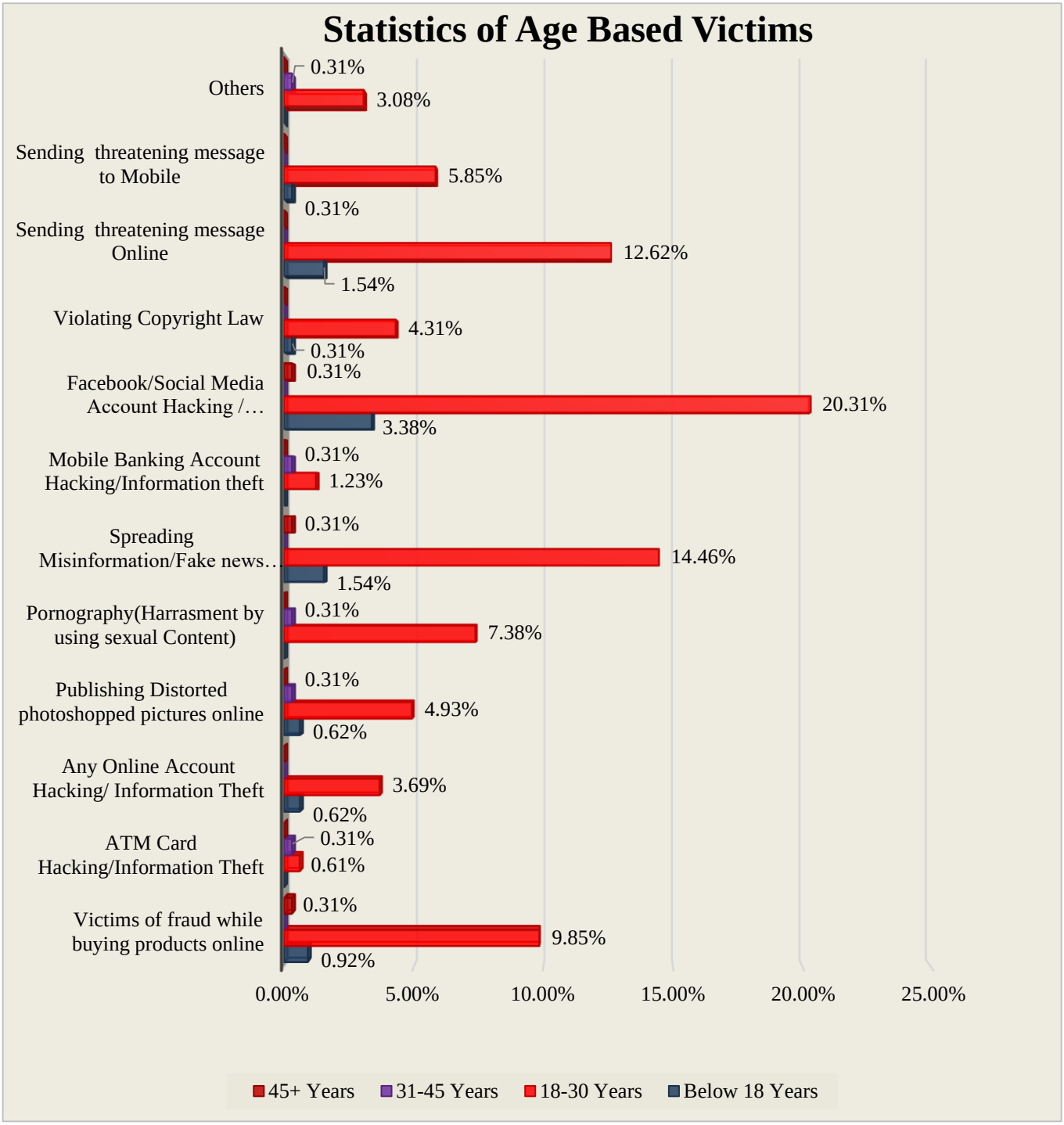
Comparative Analysis of Cyber Crime
30.00%
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
7.44%
11.08%
0.00%
0.92%
15.35%
28.31%
15.35%
5.85%
6.05%
7.69%
22.33%
16.31%
0.47%
1.54%
5.58%
4.61%
17.67%
14.16%
6.51%
6.15%
1.40%
3.39%
Victims of fraud while buying products online…
ATM Card Hacking/Information Theft
Social Media / Any other Online Account Hacking /Information theft
Publishing Distorted photoshopped pictures online
Pornography(Harrasment by using sexual Content)
Spreading Misinformation/Fake news in Social Media
Mobile Banking Account Hacking/Information theft
Violating Copyright Law
Sending threatening message Online
Sending threatening message to Mobile
Others
2018
2019-2020

5.2 Age of the Victims

During the survey, we found that most victims are between 18-30 years of age, and they make up 86.9% of the group. The second most victimised age group is under 18, and they make up 8.93% of the sufferers. Victims between the age of 31-45 beat victims over 45 by 1.8%, the former taking up 2.98% of the pie and the latter only 1.19%.

According to our survey, the first two groups, aged 18-30 and under 18, are victims of ID hacking and information theft the most.

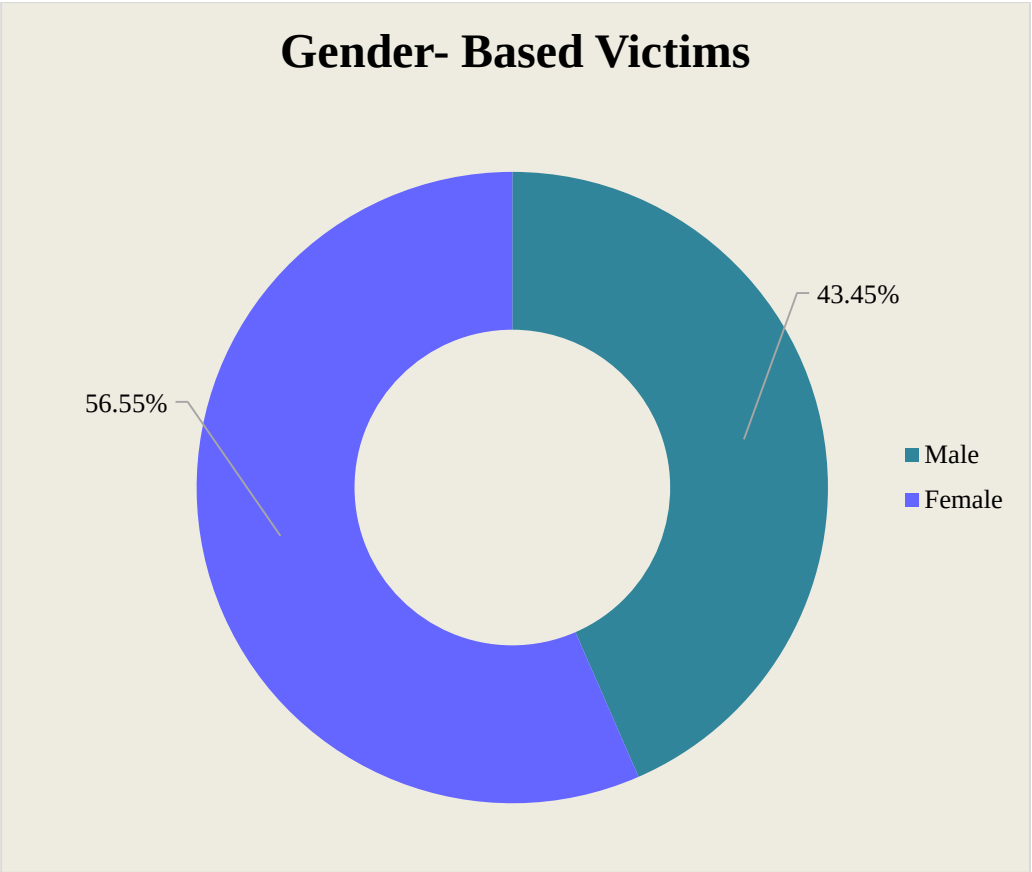


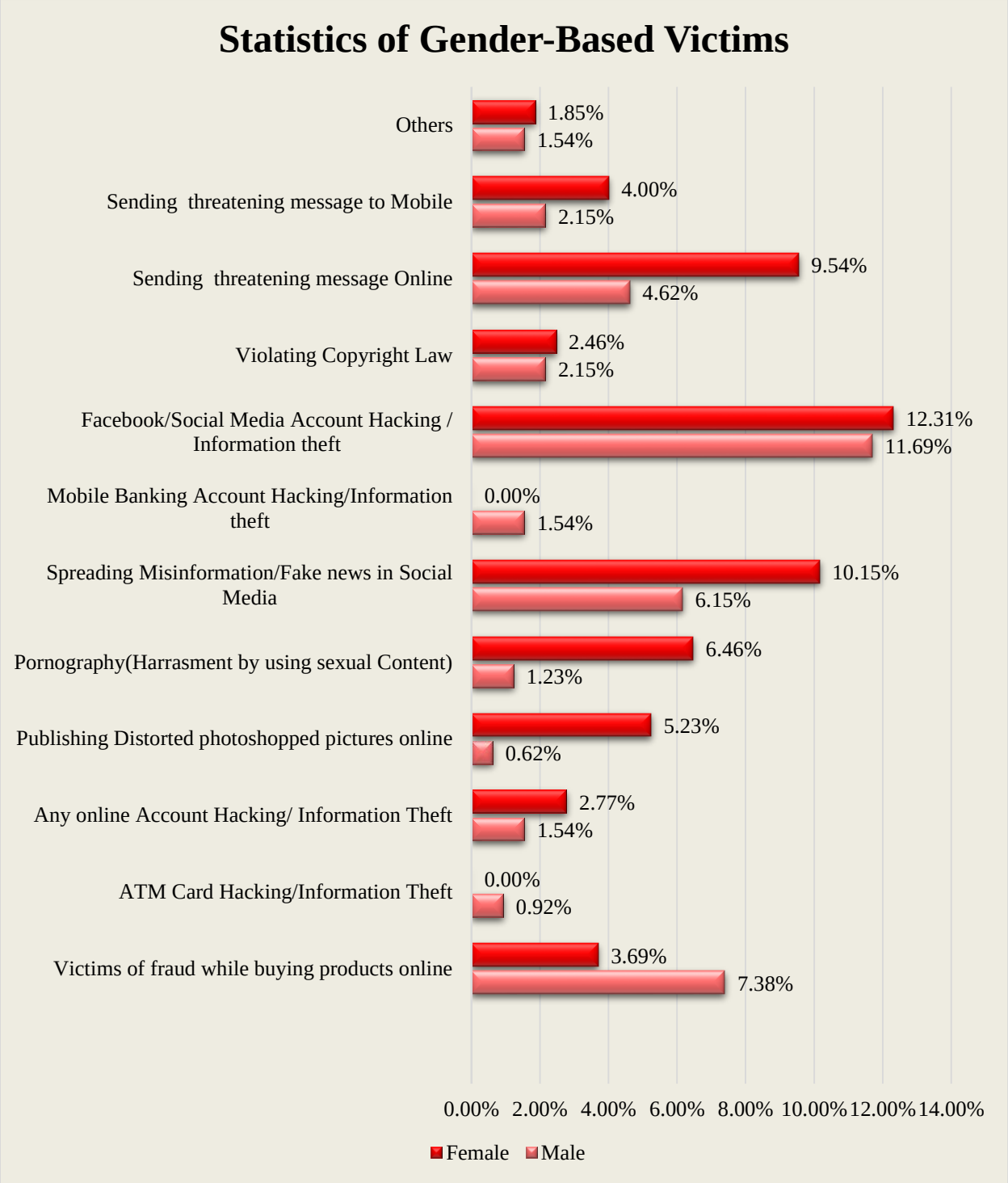

Statistics of Age Based Victims
Others
0.31%
3.08%
Sending threatening message to Mobile
5.85%
0.31%
Sending threatening message Online
12.62%
1.54%
Violating Copyright Law
4.31%
0.31%
Facebook/Social Media Account Hacking /…
0.31%
20.31%
3.38%
Mobile Banking Account Hacking/Information theft
0.31%
1.23%
Spreading Misinformation/Fake news…
0.31%
14.46%
1.54%
Pornography(Harrasment by using sexual Content)
0.31%
7.38%
Publishing Distorted photoshopped pictures online
0.31%
4.93%
0.62%
Any Online Account Hacking/ Information Theft
3.69%
0.62%
ATM Card Hacking/Information Theft
0.31%
0.61%
Victims of fraud while buying products online
0.31%
9.85%
0.92%
0.00%
5.00%
10.00%
15.00%
20.00%
25.00%
45+ Years
31-45 Years
18-30 Years
Below 18 Years

5.3 Gender-based diversity of crimes

After analysing the data, we found a difference in cybercrimes committed against men and women.

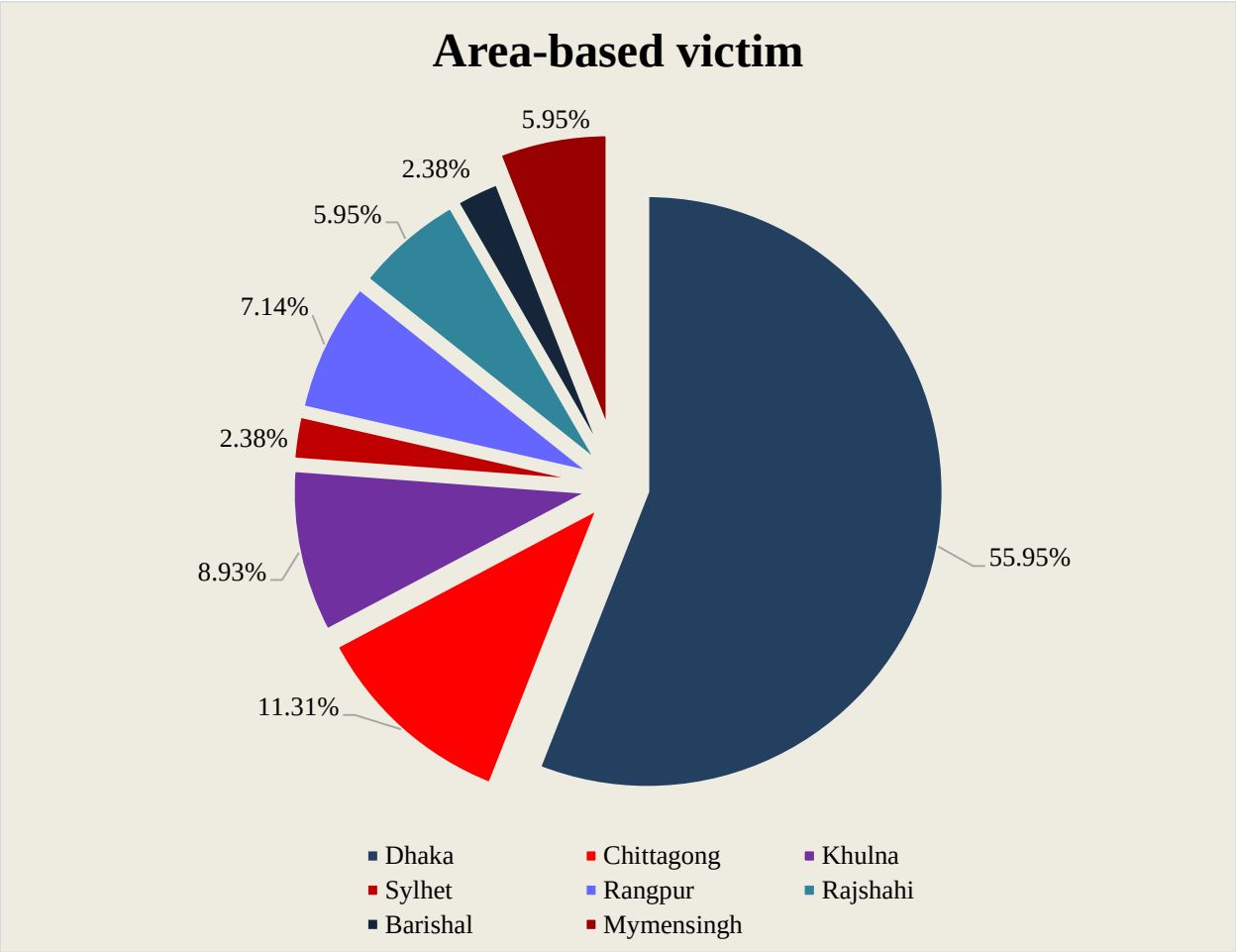
From the data we gathered, it is prominent that women are more prone to fall victim to cybercrimes than men. In our research, women victims made 56.55% of the total sample group while men occupied the other 43.45%. Also, women are more harassed on social media and face pornography-related incidents more than men. However, when it comes to online shopping, mobile banking and ATM card-related frauds, men are the primary victims of cybercriminals.




Statistics of Gender-Based Victims
Others
1.85%
1.54%
Sending threatening message to Mobile
4.00%
2.15%
Sending threatening message Online
9.54%
4.62%
Violating Copyright Law
2.46%
2.15%
Facebook/Social Media Account Hacking / Information theft
12.31%
11.69%
Mobile Banking Account Hacking/Information theft
0.00%
1.54%
Spreading Misinformation/Fake news in Social Media
10.15%
6.15%
Pornography(Harrasment by using sexual Content)
6.46%
1.23%
Publishing Distorted photoshopped pictures online
5.23%
0.62%
Any online Account Hacking/ Information Theft
2.77%
1.54%
ATM Card Hacking/Information Theft
0.00%
0.92%
Victims of fraud while buying products online
3.69%
7.38%
0.00% 2.00% 4.00% 6.00% 8.00% 10.00% 12.00% 14.00%
Female
Male

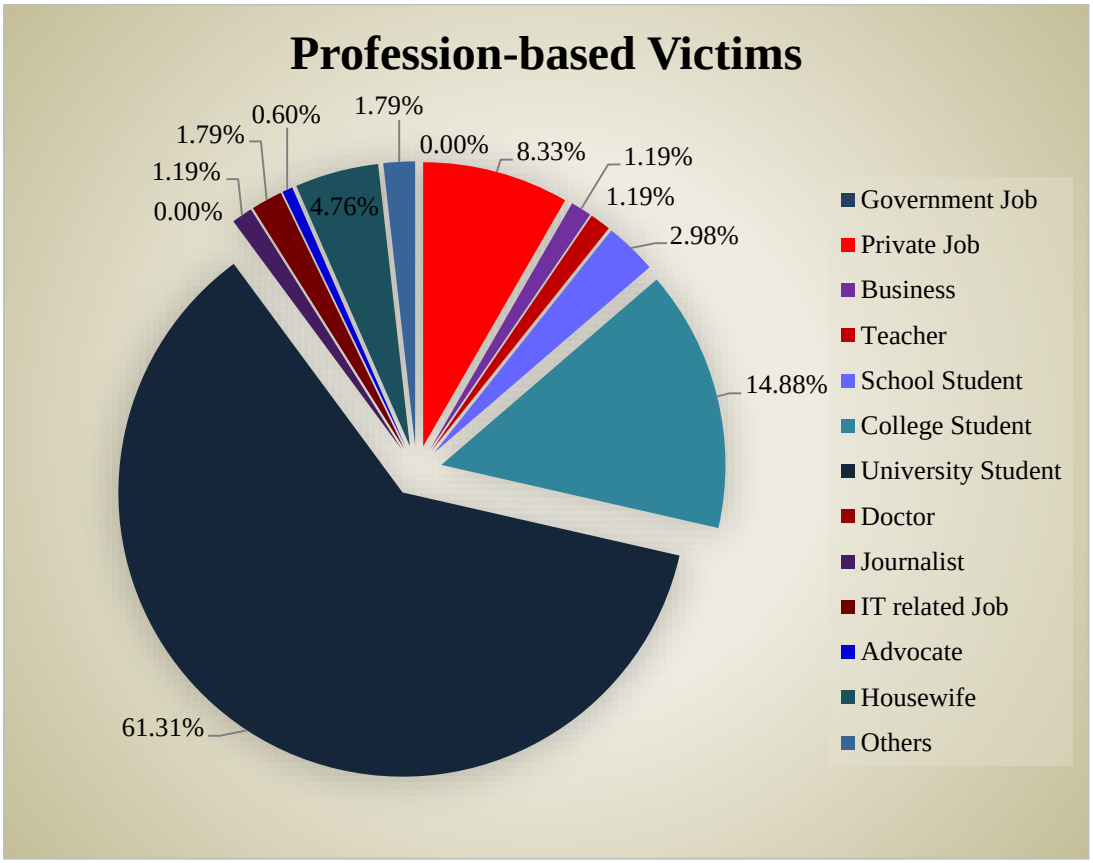
5.4 Area-based victim assessment

Location-based assessment is a fresh addition to this year's research. In our study, we found that Dhaka dwellers were the victims in 55.95% of cases, where the lowest victim count was recorded in Sylhet and Barisal, occupying 2.38% each. After further analysis, we came to the conclusion that most of the incidents of fraud and cybercrime happen in divisional cities.



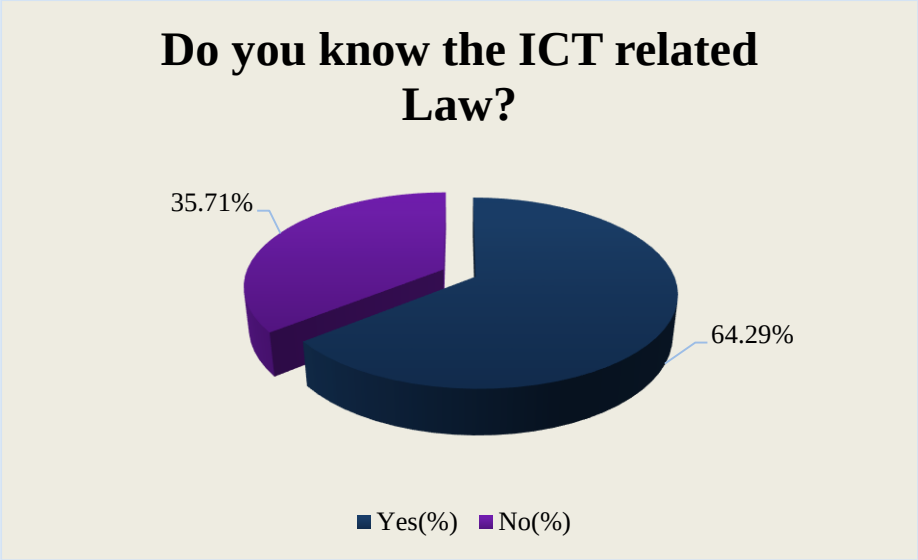
5.5 Profession-based victim assessment

Even though a profession-based assessment was not made in 2019's report, this year, after analysing the data, we found that most cybercrimes victims are undergrad students. They make up 61.31% of the total sample group, followed by college students with 14.88%, private job holders with 8.33% and journalists with only 1.19%.

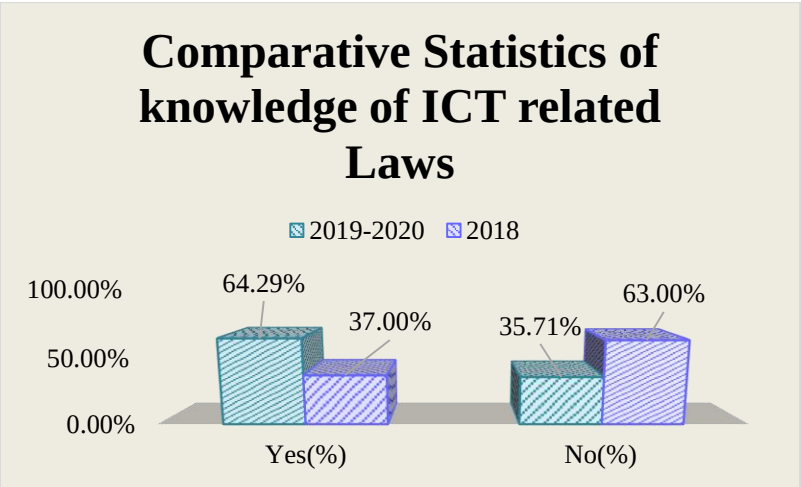


5.6 Literacy of ICT Laws

After analysing the data, we concluded that 64.29% of the victims knew ICT-related laws and regulations, where 35.71% did not have any clue.

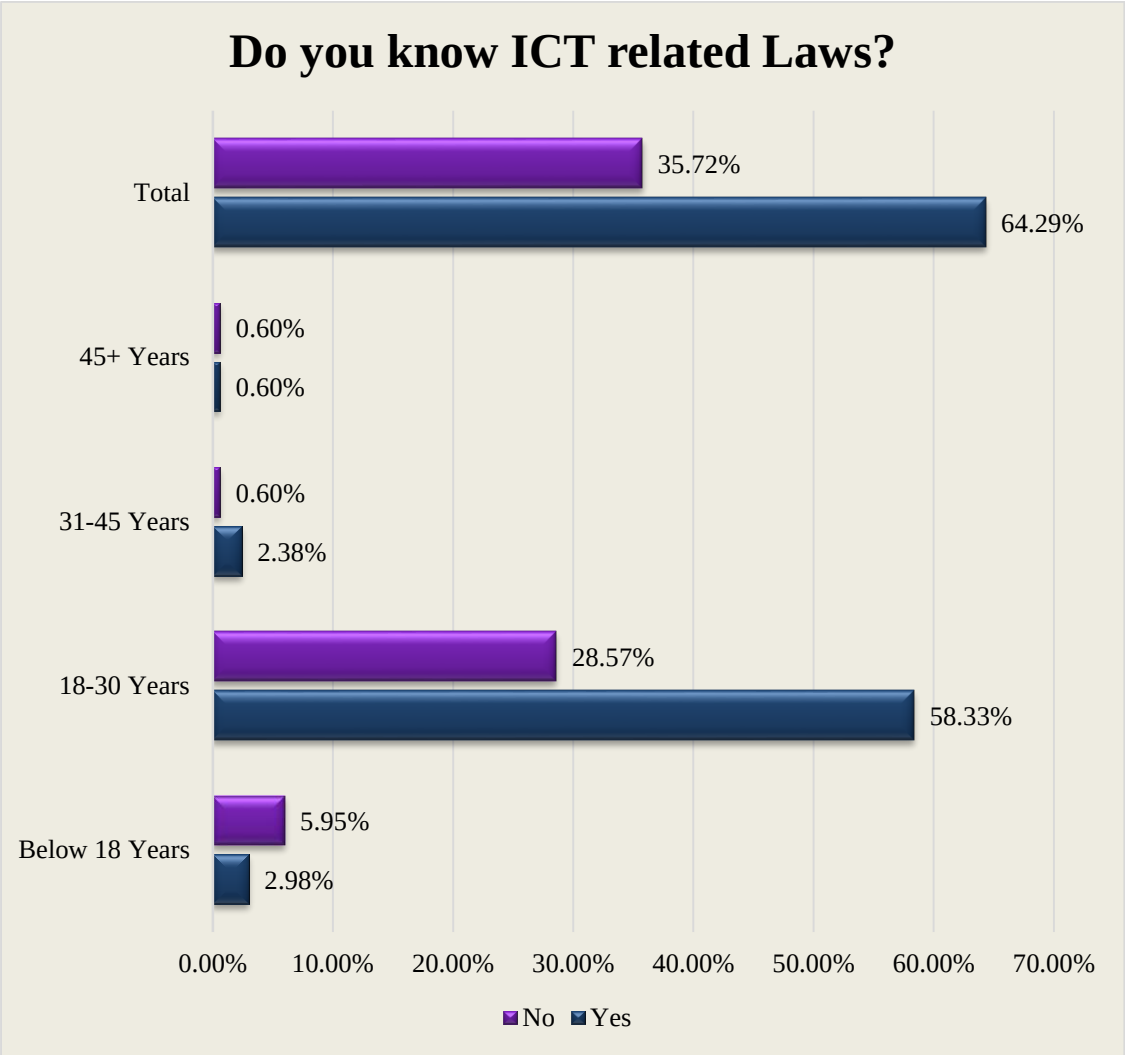


Compared to 2019's report, the number of victims with knowledge of ICT laws and regulations increased by 27.29% this year. Last year, the percentile for the learned group was only 37%, while the other group made up 63%.



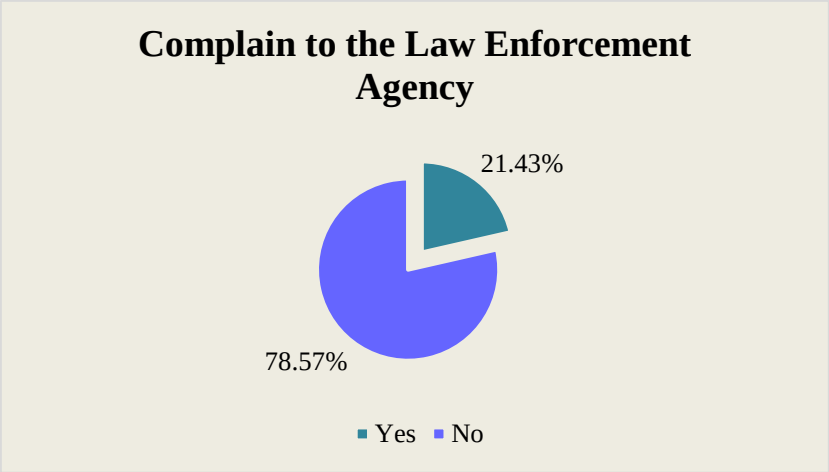
Considering age, we understood that victims of age 18-30 knew the most about local law and made up 58.33% of the focus group. People aged 45 or more were the least learned group in our study, totalling only 0.6%.

Upon looking at the number here, we realised that knowing about the laws is not enough as the 18-30 aged group, despite knowing local ICT laws, fell victim to cybercriminals the most while such crimes least harmed both 31-45 and 45+ group.

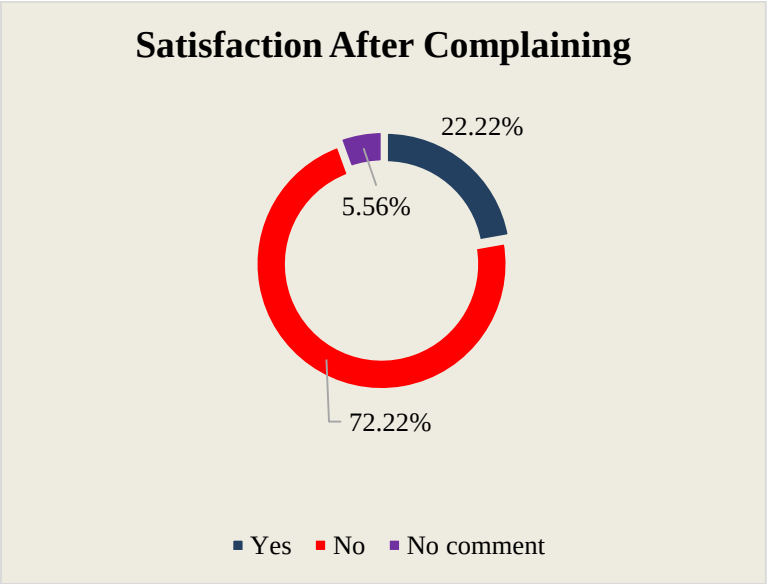


5.7 Taking help of law enforcement agencies

From the data we gathered, we summarised that only 36 out of 168 victims sought help from law enforcement agencies, which is only 21.43%.



Of those 36 complaints, only 22.22% have gotten satisfactory responses and action from the agencies, while 72.22% of victims think the actions taken against their complaints were inadequate.

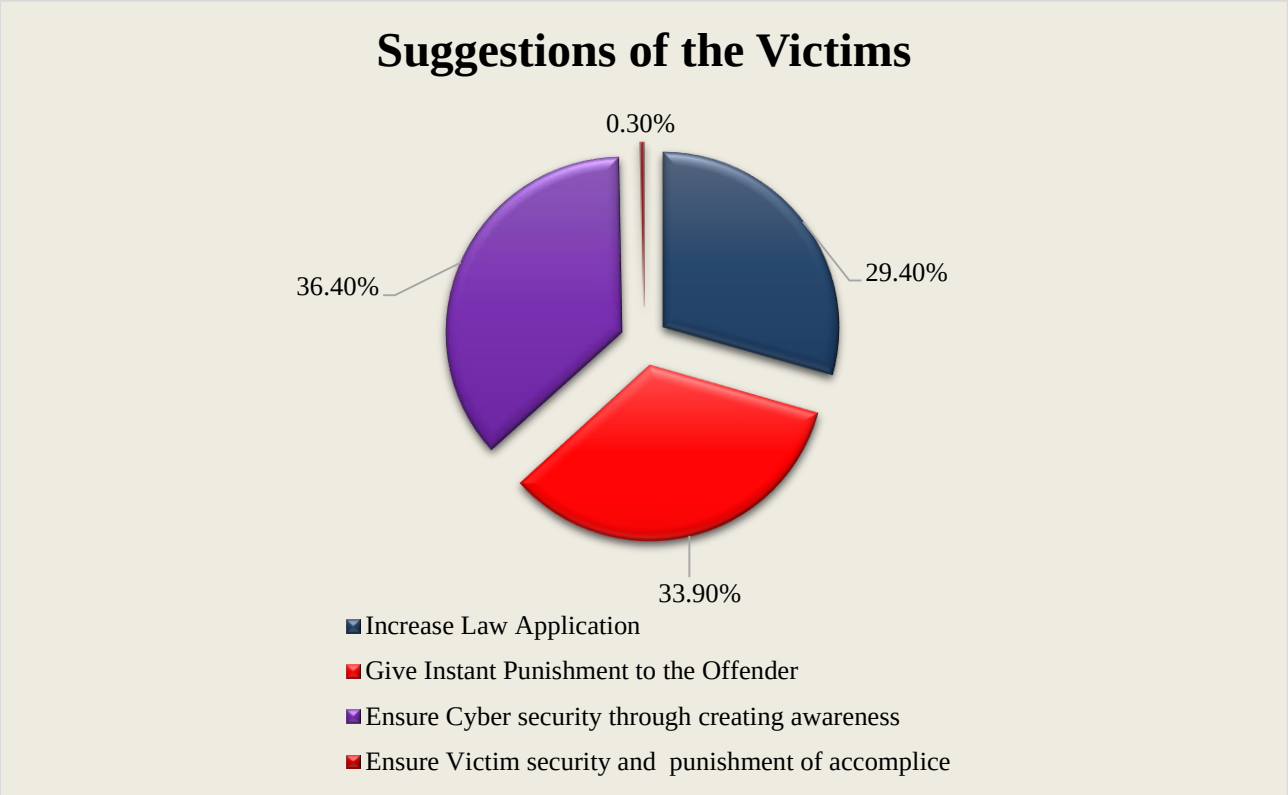


5.8 Reasons behind not taking any legal actions

Upon asking the victims, we got several reasons why they did not take lawful actions. Almost 22.2% of the victim were not sure how to approach the law enforcement agencies to file a complaint, where 20.2% thought they would be harassed by the authorities instead of getting any help. A significant fraction wanted to keep things under wrap, which is why this 18.3% did not go to law enforcement agencies. The smallest group of victims, roughly 1.2%, did not feel the need to lodge a complaint.

5.9 Suggestions of the victims

When asked about preventing cybercrimes, 36.4% suggested increasing awareness on the subject, while the smallest group of 0.3% thought victim protection and bringing criminal accomplices under the law is the way to go.



6. Advice to the stakeholders based on the assessments

Agriculture-dependent country Bangladesh is still on the path of digitalisation. Now, everyone has smartphones, and computers exist in almost every household. Information technology has really made things easier for everyone.

During the pandemic, people are embracing online life more than ever. From entertainment and education to medical treatments, everything is under the wraps of the internet, and like everything else, it comes with its own set of evils. Lack of awareness and knowledge about online activities and etiquettes often result in cybercrime, and there is no alternative to self-preservation to tackle the problem. Here are our notes to the government and relevant personnel to take a grasp of cybercrimes and ensure cybersecurity.

6.1 Independent "Cyber Squad" formation

Laws, enforcing forces and defensive equipment are not enough to ensure cybersecurity for the masses. From government and private institutions to responsible individuals, everyone must step up and work together to mitigate cybercrimes.

That is why we recommend forming a Cyber Squad that will include persons or institutions directly working with cyber space-related products and services. The squad will ideally include cybersecurity specialists, cyber police, cyber lawyers, cyber journalists, cyber businessman, cyber doctors, cyber sportspeople, cyber entertainers, volunteers, and the committee will act independently. However, the squad will be controlled centrally to ensure healthy management. If such a squad is appropriately formed and manages to work independently without any outside influence, we could see cyberspace being built that is more in line with the Bangladeshi culture. This way, people will get used to an ethical and progressive tech-fuelled lifestyle.

6.2 Spreading awareness

The masses should be made aware of cybersecurity laws through different channels. By using publication media, people should be made aware of cybercrimes, tools that are being used for such crimes, personal information's confidentiality and how the judiciary system handle these offences.

Nowadays, these messages can be broadcasted to the masses very easily:

6.2.1 Mass Media

Mass media is considered to be the mirror of any society that plays a pivotal role in building perception. It would not be a stretch to say the media form public opinion on a subject. That is why, to spread awareness about cybercrime and criminals, the media's help is a must. The damaging character of the cyber world and preventative measures should be publicised through the use of mass media.

6.2.2 Educational Institutions

From an early age, kids should be made aware of the negative aspects of the cyber world. In this prospect, the educational institutions will have to play a pivotal role. Textbooks need to include the negative sides of having technology in our grasp along with the benefits we reap from it. Seminars can be arranged in educational institutions to help students get through internet addiction. As a healthy alternative to violent games, physical sports and the importance of family bonding must be taught.

6.2.3 Initiatives by Government and private institutes

Both government and private institutions need to take necessary preventive steps in order to spread awareness among the mass and to build a healthy cyberculture.

6.3 Accessibility of legal help

From the research, it is clear that not everyone is caught up with local laws regarding information technology. Almost 35.71% of the victims in our sample group were unaware of the rules and regulations. Since legislative language is not colloquial, people often find it difficult to read into it. That is why it is essential to simplify the language or create simple explainer videos on essential laws and passages. Once people understand the rules and regulations, they will be assured of their rights and take necessary action against cyber offences. At the same time, people will realise the consequences of the crimes and avoid being involved in such incidents.

6.4 Increase efficient personnel in law enforcement agencies and gain the trust of people

Proper steps should be taken to increase the efficiency of law enforcement agencies' actions. Since the type, method and tools used in cybercrimes frequently evolve, it becomes difficult to catch the culprit with every passing day. That is why a dedicated cyber branch should be sanctioned in all police stations.

In this research, we found out that only 21.43% of all victims take help from the law, and even in this small group, 72.22% of the complainers did not get a satisfactory response. From the fear of harassment, 20.20% did not even bother to lodge a complaint. Looking at the numbers, it is clear that people are not happy with how law enforcement agencies handle the cases now. The lack of mistrust prevents people from getting necessary help which should be fixed as soon as possible.

6.5 Proper utilisation of political members

The human resources of political parties in Bangladesh can play a crucial role in developing healthy cyberculture. Since political leaders preside over critical social events, having them spread awareness might be the most efficient way to ensure the message reaches the farthest corner. For that, union and local young and experienced politicians can be trained on cybersecurity and awareness. Later these trained individuals can help bring positive change to society.

6.6 E-commerce policy & controlling authority

Appropriate safeguards should be implemented to protect the booming e-commerce sector against fraudulent activities. Thankfully, the Ministry of Commerce is already working on a draft of e-commerce policies which is the right step forward. However, the ministry already worked on a "Digital Commerce Policy", which was approved in the cabinet, and the ministry is yet to assign a governing authority to oversee the sector. That is why approval for the new policy is so vital for the betterment of this sector.

Open delivery, unsatisfactory product return, cash on delivery and "no payment before seeing the product" – these policies should be ensured on the draft to completely mitigate e-commerce fraud and make businesses focus on customer satisfaction.

6.7 Remedy of porn addiction

Of all the evils in the cyber world, pornography is definitely the most hated and vicious crime. Due to the widespread availability of such adult content, women are being molested every day, and the youth of the country is slowly slipping from their moral ground.

Our youth must be safeguarded from this heinous and perverted grasp of pornography. To do so, the practice of healthy culture, implementation of local law and religious influence can prove to be most effective.

6.8 Cybersecurity ensured for women and children

Both men and women fall victim to cybercrime, but the most sensitive recipients of such offence are women and children—that is why crimes against children and women must be dealt with utmost importance. Also, specific awareness programs must be arranged to help these two groups. Proper implantation of the law and exemplary trials can also help lower the cases revolving around women and children.

6.9 Building efficient staffing in the cybersecurity sector

Bangladesh must emphasise cyber training to catch up to the exponential growth of the cyber world. Commercial institutions must build a dedicated cyber team and train them to strengthen cybersecurity. That is why both government and private initiatives for setting international standard training centres to output cybersecurity engineers should be expected. Separate multipurpose research facilities should be built so that our trained and efficient workforce can be exported to other countries, bringing remittance and ensuring jobs overseas.

7. Conclusion

The world is dependent on ICT. Undoubtedly, the Digital Bangladesh vision triggered digitalisation and simplified people's daily needs and tasks. However, ICT and digitalisation also affected us adversely in many ways. Building an independent Cyber Squad with "Responsibility of building a cyber-safe nation is upon all" as the motto can help form safe and healthy cyberculture in the country.