TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technologies

Mohammed Jasim Uddin 177772IVSB

Evaluating Cyber Security Situation in Bangladesh: Inclusion of information security in secondary education

Bachelor’s Thesis

Supervisor: Edmund Laugasson
Master of Science (MSc)

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Mohammed Jasim Uddin 177772IVSB

Küberjulgeoleku Olukorra Hindamine Bangladeshis: Infoturbe Kaasamine Keskharidusse

Bakalaureusetöö

Juhendaja: Edmund Laugasson

Master of Science (MSc)

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Mohammed Jasim Uddin

07.01.2021

Abstract

There has been a lot of interest in cybersecurity lately, mainly due to the fact that people are being exposed to new cyber threats as days come by. The complexity of cyber threats has always interested the researchers of this field to invent new ways for tackling the problem. Most of the solutions considered increasing security on the manufacturer end (of software and microchips), but educating the mass people was always overlooked, especially in a country like Bangladesh where the internet has become well accessible with the reduction of price in smartphones and mobile data. Hence it poses a great threat to the uneducated percentage of people of the country. This dissertation takes the demography of internet users in Bangladesh into account and advises a comprehensive solution that will help tackling the problem of cyber threats and bullying.

Bangladesh faces several types of cybercrimes throughout the year, most of them are phishing, online income scams, pretexting, etc. Ransomware attacks are also common with computer users. The main reason for people falling victim to these crimes is their lack of knowledge of cybersecurity. Hence our proposal of including a course in cybersecurity in secondary level education stands justified and that hypothesis has been proved later on in the dissertation.

The survey conducted proves the claim that once a simple course in cybersecurity gets introduced in the school, it is believed to enhance the knowledge of the students who are usually deprived of any idea on cybersecurity in the secondary or junior level.

This thesis is written in English and contains 41 pages, including 5 chapters, 45 figures, and no table.

Annotatsioon

Küberjulgeoleku Olukorra Hindamine Bangladeshis: Infoturbe Kaasamine Keskharidusse

Viimasel ajal on küberturvalisuse vastu olnud suur huvi peamiselt seetõttu, et üha enam puutuvad inimesed kokku uute küberohtudega. Küberohtude keerukus on alati huvitanud selle valdkonna eksperte, et leida uusi võimalusi probleemide lahendamiseks. Enamik lahendusi tehti turvalisuse suurendamiseks tootjate poolt (tarkvara ja mikrokiipide osas), kuid suurema hulga kasutajate harimine jäi alati tähelepanuta, eriti sellises riigis nagu Bangladesh, kus internet on nutitelefonide ja mobiilse andmeside hinna alandamise kaudu muutunud hästi kättesaadavaks. Seega kujutab see suurt ohtu harimata osale riigi internetikasutajatest. Käesolevas töös võetakse arvesse Bangladeshi internetikasutajate demograafiat ja soovitatakse terviklikku lahendust, mis aitab küberohtude ja kiusamise probleemi lahendada.

Bangladesh seisab kogu aasta jooksul silmitsi mitut tüüpi küberkuritegudega, enamik neist on andmepüük, veebipõhised sissetulekupettused, erinevad petuskeemid jne. Lunavararünnakud on tavalised ka arvutikasutajatele. Nende kuritegude ohvriks langemise peamine põhjus on teadmiste puudumine küberturvalisuse alal. Seetõttu on meie ettepanek lisada küberturvalisuse kursus keskharidusse õigustatud ja hüpoteesid on hiljem käesolevas töös tõestatud.

Läbiviidud küsitlus tõestab väidet, et kui koolis on hakatud tutvustama lihtsat küberturvalisuse kursust, siis arvatakse, et see suurendab nende õpilaste teadmisi, kellel tavaliselt puudub igasugune teadmine küberturvalisuse kohta kesk- või nooremas kooliastmes.

See lõputöö on kirjutatud inglise keeles ja sisaldab 41 lehekülge, sealhulgas 5 peatükki, 45 joonist ja 0 tabelit.

List of abbreviations and terms

PC	Personal Computer
IT	Information Technology
IP	Internet Protocol
NASA	National Aeronautics and Space Administration
RAT	Remote Access Trojan
BTRC	Bangladesh Telecommunication Regulatory Commission
CERT	Computer Emergency Response Team
NCSS	National Cyber Security Strategy
R&D	Research and Development
OWASP	Open Web application security project
ICT	Information and Communication Technology

Table of contents

List of Figures

1. Introduction

We live in an advanced time that comprehends that our private data is more vulnerable than at any time in recent memory. The whole world is living together, from web banking to government framework, where information is put away on different gadgets. That is why the internet is turning out to be popular day by day. Being encouraged with its goodness, individuals can impart effectively just as a global level. Nowadays we can get any information from the internet. A part of that information can be sensitive data, regardless of whether that be licensed innovation, money related information, individual data, or different sorts of information for which unapproved access or introduction could have negative results. Despite the fact that it is the most straightforward method of connecting to people, presently it is a matter of worry that abuse of PC (Personal Computer) and web setup certain individuals to carry out violations. Among the various wrongdoings in the present society; cyber-crime has become just as extremely devastating. In addition to the fact that casualties should report such doubt or potential wrongdoing, yet the casualty needs to recognize the presumed machine so police can take proper steps. Without having the PC structure in which the culprit carried out his crime(s) at that point it is difficult to convict and mistreat these culprits. Casualties of cybercrime need to get mindful of such wrongdoings and they have to turn out to be more taught in how to secure and forestall themselves as well as others too from such acts.

Cybersecurity is the insurance of internet-associated frameworks, including equipment, programming, and information from digital assaults. It is composed of two words; one is digital and the other is security. Digital is identified with the innovation which contains frameworks, organizations, and projects or information. While security is identified with the assurance which incorporates frameworks security, network security and application and data security[1]. Likewise, we can characterize network safety as the arrangement of standards and practices intended to secure our processing assets and online data against dangers. Because of the weighty reliance on PCs in a cutting-edge industry that stores and communicates a plenitude of classified and fundamental data about the individuals, network safety is required for protection.

It is good for us that various government organizations around the globe have played an important role to recognize and aggrieve culprits of cybercrime. Despite the fact that, in light of the tremendous measure of innovation being produced routinely government offices need to remain ready and educated to control cybercrime. In Bangladesh, the Government should take some great steps to fight cybercrimes including education about information security[2].

In this thesis, we will deal with the problem regarding cybercrimes and we will propose some steps to minimize the loss because of it. We will also focus on the following goals-

- Increasing social awareness about cybercrimes.
- Gaining sufficient knowledge about information security.
- Preventing more cybercrimes in the future.
- Important information will be protected.
- Minimizing the loss caused by cybercrimes.
- Acknowledging privacy importance and start using it as much as possible

2. Background Study

For our study in cybersecurity evaluation in Bangladesh, first, we need to know about the cybercrime situation, reasons, classification, and the law about those who commit it. Then we can propose the steps to include education about IT (Information Technology) based on our survey.

Now we will learn about the classification of cybercrimes and the types of criminals who conduct those. There are mainly two kinds, one is web-based and the other is system-based attacks. We can also divide them based on users. Then we will discuss about the cybercrime situation in Bangladesh, what are the reasons behind those, and last but not least we will describe a basic knowledge about cybersecurity laws in Bangladesh.

2.1 Classification of Cybercrimes & Cybercriminals

There are different types of cyberattacks, but firstly we can divide them into two types. One is Medium Based attacks, and the other is User based attacks.

Medium based attack indicates those attacks where the attacks were conducted via a medium like a website or software. So, we can divide this into two parts. One is web-based attacks and the other one is software-based attacks[3].

On the other hand, a User-based attack clearly indicates the attacks which were performed by targeting the user(s) or a community[4]. On that basis, it can be divided into four parts. Those are-

- Cybercrime against individuals.
- Cybercrime against individual property.
- Cybercrime against organization.
- Cybercrime against society at large.

So, if we want to demonstrate the classification, it will look like the following figure.

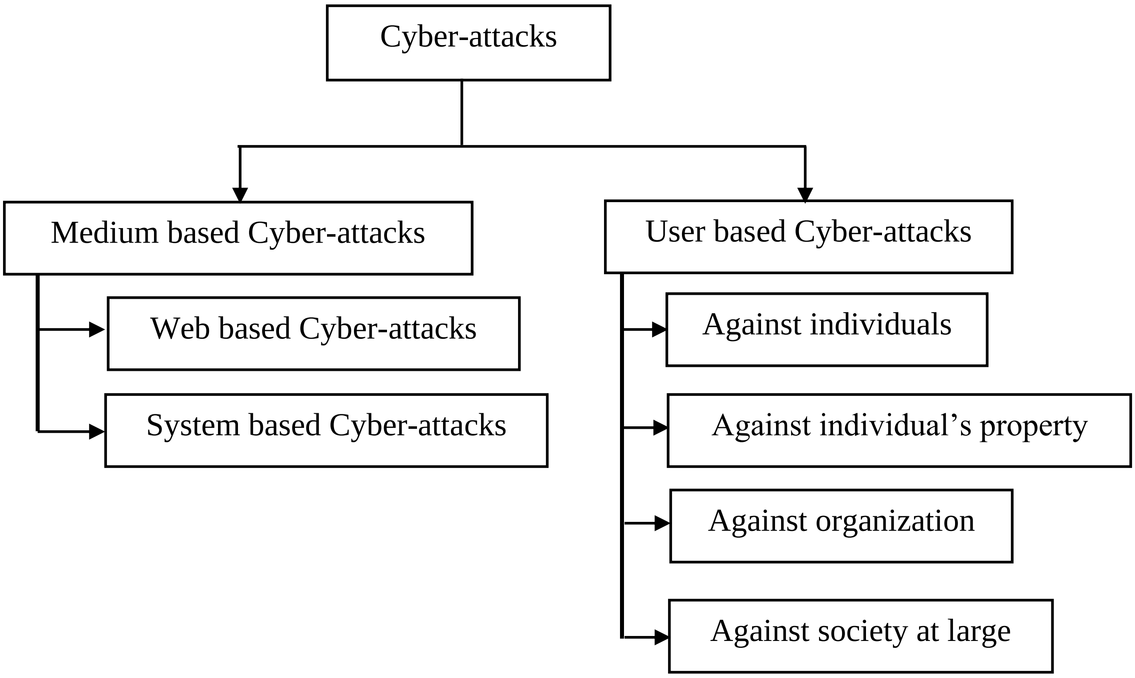


Figure 1. Classification of Cyberattack

2.1.1 Categories of criminals

This section will discuss about the categories of cybercriminals. The cybercriminals can be divided into different groups/categories. This division may be justified based on the object that they have in their mind. The following are the category of cybercriminals-

Children and adolescents between the age group of 6 – 18 years: The basic explanation behind this sort of deficient personal conduct standard in youngsters is seen generally because of the curiosity to know and investigate things. Other related explanations might be to demonstrate themselves to be exceptional among other youngsters in their gathering. Further, the reasons might be psychological even.

Organized hackers: These sorts of programmers are generally coordinated together to satisfy certain targets. The explanation might be to satisfy their political inclination, fundamentalism, and so forth The Pakistanis are supposed to be extraordinary compared to other quality programmers on the planet. They chiefly focus on the Indian government locales with the reason to satisfy their political goals. Further, the NASA (National Aeronautics and Space Administration) just as the Microsoft locales is consistently enduring an onslaught by the hackers.

Professional hackers/crackers: Their work is propelled by the shade of cash. These sorts of programmers are generally utilized to hack the site of the opponents and get trustworthy, dependable, and significant data. Further, they are utilized to break the arrangement of the business essentially as a measure to make it more secure by recognizing the loopholes.

Discontented employees: This group incorporates those individuals who have been either sacked by their manager or are disappointed with their boss. To retaliate for they typically hack the arrangement of their worker.

2.2 Cybercrime in Bangladesh

In Bangladesh, people are less aware of cybercrimes[5]. They are not familiar with these types of crimes. There are several types of cybercrime that occurred in Bangladesh which are being mentioned [6]. Example-Steganography, Cyber Defamation, Email Bombing, Phishing, Pretexting, Online Income Scam, Backdated Technology in Organization, Giving Access to Info While Installing App, Games or Software Download from Unauthorized Source, Giving Info to Get Access or Download Something, sharing all personal info to the Internet, Filming sexual assault.

Cyber-attacks often took place, which caused loss of assets in a very recent time. With the increasing number of internet users, the number of attacks ratio is also going up. According to the Kaspersky Security Bulletin 2015, Bangladesh is in the second position in the level of infection among all the countries. 69.55% of unique users are at the highest risk of local virus infection in Bangladesh. 80% of users are the victim of spam attacks according to Trend Micro Global Spam Map.

Since the largest cyber heist in the history of global financial forgery, the Bangladesh government took the issue very seriously, considering its damage to the economy, and formed an anti-cyber attack unit called 'cyber incident response team' (CIRT). The government formed the CIRT Bangladesh e-Government Computer Incident Response Team (BGD e-Gov CIRT) under the Bangladesh Computer Council (BCC) just after the incident of Bangladesh Bank's reserve heist took place. It was formed to combat any such fatal intrusions further. According to state-run BGD e-Gov under the Ministry of Posts, Telecommunications, and Information Technology. Figure 2 illustrates the incident reporting statistics for recent years. It is clear that cyber-attacks in Bangladesh increasing day by day.

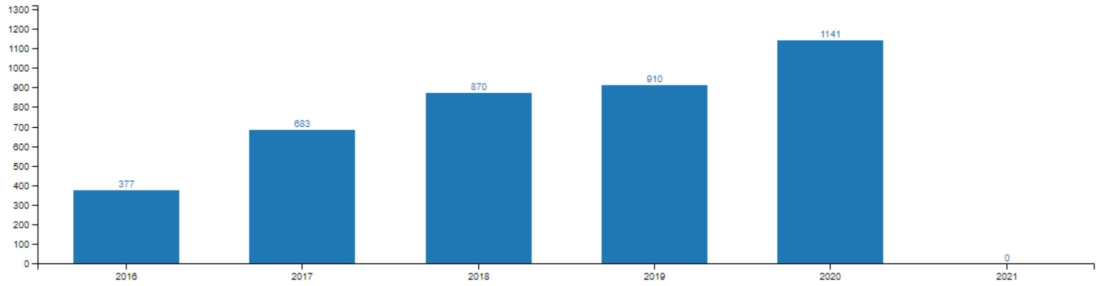


Figure 2. Registered incident per year [7].

The incidents registered with the organization increased to 870 in 2018 from 683 in 2017 and reached to 1141 incidents in a year by 2020[7].

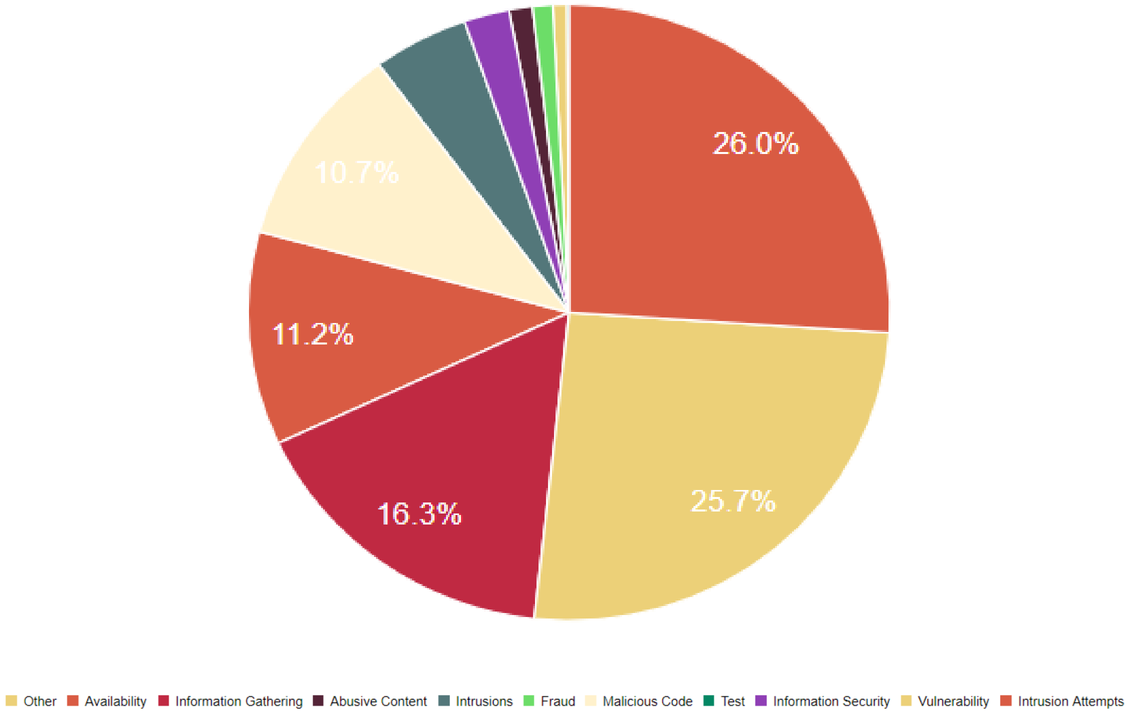


Figure 3. Incident classification [10].

Of the attacks, vulnerability accounts for 25.6 percent, intrusion attempts 25.8 percent, information gathering 16.8 percent, malicious code 10. 6percent and the rest comprise fraudulence, service request, fraud, availability, intrusion, test, abusive content, information security, and others[7]. But the actual number of attacks is much higher.

Figure 4 describes the factors influencing the incidents that have been listed by the CIRT team of the Bangladesh gov. As per the statistics, vulnerability is mostly caused by a vulnerable system. Other than this there are also some other significant factors which are infected system, c2 server, scanning(social engineering), DDOS, login attempts, exploitation of known vulnerabilities. Most of these vulnerabilities are mentioned in OWASP as a top 10 web application vulnerabilities [8].

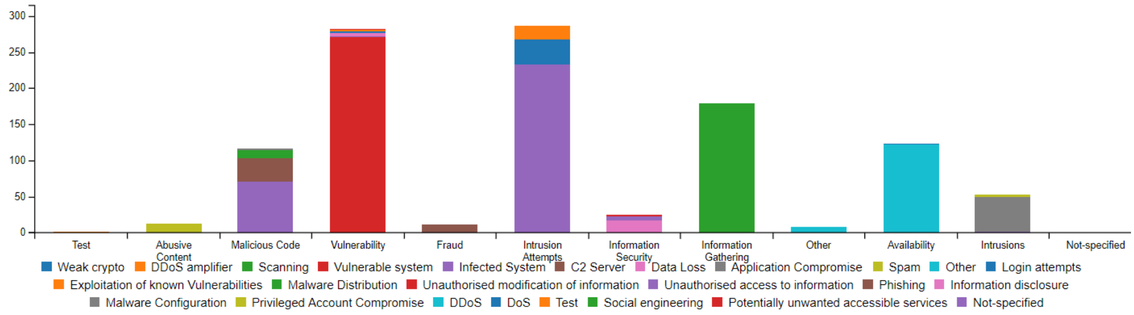


Figure 4. Types of Incidents [7].

2.3 Reasons for Cybercrime in Bangladesh

There are plenty of reasons which lead a person to commit cybercrime[9]. But there are some which mostly caused that. Some of the reasons are mentioned below-

Unauthorized access: The issue experienced in guarding a computer framework against unapproved access is that there is a chance of penetration not because of human mistakes however because of the complexity of the technology. By secretly implanted logic bombs, keyloggers that can steal access codes, advanced voice recorders; retina images, etc. that can fool biometric systems and bypass firewalls can be used to move beyond numerous security systems.

Negligence: Negligence is very connected to human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber-criminal to gain access and control over the computer system and do whatever they want.

Loss of evidence: Loss of evidence is a very common & obvious problem as all the data are routinely destroyed. A further collection of data outside the territorial extent also paralyzes this system of crime investigation.

Expertise of criminals in technological issues: In the vast majority of the occasions, the criminal used to be profited by doing cybercrimes. But sometimes they commit a few wrongdoings just to show their skill and cross-check their insight. Despite the fact that they do not pick up anything besides they fall inside its dependence.

Misuse of computer and information technology: Bangladesh is undergoing technological up-gradation countrywide. The govt. Vision Digital Bangladesh by 2021 is another accelerator to meet the target. So, the use of computers and Information Technology expanded highly which broadened the scope of cyber criminality. As it opens the scopes of more crime if the people are not well-educated about this.

Indefinite Legal Jurisdiction: Most internet crime takes place across international borders. Law enforcement agencies are always limited to jurisdictional boundaries. For instance, a city police officer in Bangladesh cannot easily arrest someone in another country. For that, international criminals have no fear about that. Also by collaborating with other countries and catching the criminal will take so much valuable time that they can escape easily[10].

Lack of Knowledge: Barely any casualties of cybercrime have the assets, innovation, or subsidizing to seek after the culprit. Because mostly they do not want anyone to know about it and they think that will decrease their social status. Only the persons knowing about cybercrime and cybersecurity will step forward without that social status. The essential information shows that numerous individuals have lost a lot of money to false exchanges, including vehicle deals, stock exchanges, bank moves, etc. Tragically, the amount lost usually pales contrasted with the expense of the assets that would be expected to recover the assets.

2.4 Cybersecurity Laws in Bangladesh

There are insufficient laws in Bangladesh that may punish the cybercriminals. In Bangladesh court, there is a law named "The Bangladesh Information and Communication Law 2006" (As revised in 2009) In this law area 56(1) has announced the punishment of 10years of detainment with or without a fine.

Section 68 of the said act has pronounced the development of a special council named "Cyber Tribunal". Who may take perception of such sorts of Cyber Crime however it still cannot seem to forestall or rebuff the criminals.

Because of the shortage of trained specialists assisting the court, it has gotten more difficult for the judge to follow the wrongdoings. There is just a digital court in Dhaka City set up under Section 82 of the said act. This council has not yet awarded any discipline to any crook. Out of this till to the foundation of Cyber Tribunal in the region court the Session Judge has the comprehension to preliminary such sort of wrongdoings[11].

Over the last six years, some 3,659 cases related to cybercrime have been lodged in Bangladesh. Of them, 1,575 cases went to the Cyber Tribunal that was established on 28 July 2013. According to the Police’s Crime Data Management Systems, only 522 cases were settled, and criminals were punished in only 25 cases[12].

In Bangladesh, there is a legal authority named BTRC (Bangladesh Telecommunication Regulatory Commission) which proceeds as a protector in digital insurance, yet it is to satisfy its promises. It has the authority to conduct mobile courts with the help of other government organs for the quick trial of such kind of crime.

The offenses of the Bangladesh Information & Communication Technology Act 2006 are non-cognizable under section 76(2). The victim has to file an allegation to the law enforcing agencies to get a remedy. This is the main weakness of the said act. At the time of enactment of the said Act, it was said in section 68 that a special tribunal named Cyber Tribunal will be established in every district of Bangladesh. But till now only a tribunal has been established in Dhaka City.

The Bangladesh police have a special branch named "Anti-cyber–Crime Department " headed by the Deputy Commissioner of Police to protect against e-mail fraud, treat by email, defamation, or publishing of unauthorized pictures. But the department is yet to fulfill the public demand due to the scarcity of well-trained manpower[13].

To secure and follow the cybercriminals around the world, the Computer Emergency Response Team (CERT) is the most effective technique. It comprises digital authorities everywhere in the world. The function of CERT is to monitor the computer network of the world. At the point when any interference, abnormalities, or any sort of unlawful exercise happened CERT can think about it. Thinking about it vital advances are taken to ensure or forestall the wrongdoings. By this, no event of an organization is obscure to CERT. Bangladesh has formed the authority of CERT by taking authorization from the global CERT.

But the government is yet to permit this. For this, it is working only for the necessity of an international CERT. As indicated by the experts of Bangladesh if the administration allows the approval of CERT of Bangladesh each event will be followed by the law implementing organizations. For these situations, the wrongdoings might be followed at the underlying stage and afterward, a legitimate implementation might be taken without any problem. Then again, taking activities as per the law may get simpler on account of taking contingencies and recording any case. As cybercrimes can be followed in fact by the authority of Bangladesh and vital information can be guaranteed by the Bangladeshi for this a professional group of CERT can be shaped for the more prominent advantage of the individuals of Bangladesh[14].

2.5 Literature Review

In April 2019 Kaushik Sarker, Hasibur Rahman, Khandaker Farzana Rahman, Md. Shohel Arman, Saikat Biswas, Touhid Bhuiyan performs[15] a cross-comparison on the National Cyber Security Strategy (NCSS) of a country (Bangladesh) with the most technologically advanced countries like the USA, Japan, Malaysia, Singapore & India. As they already mentioned some terrible incidents related to cyber-crimes, they proposed some legal measures to increase cybersecurity in Bangladesh. They focused on some Important comparison criteria which include promoting cybersecurity R&D (Research and Development) and education, risk assessment & counter cybercrime policy, institutional aspects & balancing cyber securities with civil liberties. They also showed that Bangladesh partially has some of the measures and most of them are absent and those are in the document. So, they suggested implementing those properly. The main drawback of their research was based on the cross-comparison of different countries, but they do not know if those strategies will work for Bangladesh or not. In February 2018 Shusmoy Kundu, Khandaker Annatoma Islam, Tania Tahmina Jui, Suzzana Rafi, Md. Afzal Hossain, Ishraq Haider Chowdhury analyzed[16] cyber attacks happening in recent years. They investigated cybercrimes focusing on financial sectors in Bangladesh. They also describe some of the global scenarios of cybercrimes and statistical data of investment in cybersecurity of other countries & organizations. They focused on the banking sector because it is the most vulnerable option. They demonstrated the risk percentage of different banks' cybercrime in Bangladesh. They also suggested some ways to minimize the loss for cybercrimes such as Investments in cybersecurity aspects, legal framework, seminar and training, computer emergency response team formation, cybersecurity strategy, code of ethics, etc. Another research, conducted by Md Nurul Afser Siddique, is also focused on cybersecurity risk mitigation of financial organizations in Bangladesh. The main drawback of their analysis was they only focused on the financial sector, but cybercrimes are also a big threat to other sectors. Those sectors are also important, and we can`t ignore them. A financial strategy may not work for other sectors.

In October 2014 Mohammad Nur Nabi & Muhammad Tanjimul Islam attempted[17] to describe the threat of cybercrime in the globalized world with an emphasis on Bangladesh. At first, they indicate how vulnerable it is as the Bangladesh government uses foreign servers & vendors. Also, nowadays almost everything is online-based, so it is now more vulnerable. They also pointed out the difficulties and to overcome them they suggested some measures. They categorize cybercrime into four (4) and prevent each one of those into different methods. The measures they suggested are like reform legal structures, maintaining rules of cybersecurity, individual awareness. Their drawback was they didn`t describe properly and elaborately how those measures could be taken & benefit us.

In the perspective of Bangladesh, cybercrime is a new concerning issue for Bangladesh. Bangladesh's government has introduced the Information and Communication Technology Act 2016. In the act, areas 56,57,66,67 portray the way and exercises of cybercrime. Though the government introduced the act with lots of hope, it has some major drawbacks[14], they are listed below:

- According to the act, police have the power to arrest anyone without any warrant. There is a high possibility of misusing power as the police in Bangladesh are politically biased. This may increase harassment to the general internet users and arbitrary arrest by police.
- It was mentioned in the ICT act that a cyber-tribunal will be established all over the country but only a few courts have been established. As a result, it cannot provide adequate justice for the victims of cybercrimes.
- For the investigation and detection of cybercrime and criminals, there is no digital forensic laboratory in our country.
- Police hardly have adequate knowledge and training to investigate cybercrimes and collect evidence. As a result, real criminals often do not get arrested.
- The government has failed to reach the mass people and the majority of illiterate people of Bangladesh do not know the existing ICT act.

There are some other laws introduced by the government such as the Pornography act 2012, Bangladesh Telecommunication Act 2001, Digital Security Act 2016. But the government has failed to enforce the laws properly and thus the rate of cybercrime is increasing day by day. Many educated people have no idea about these acts let alone illiterate and poor people. Raising awareness about existing cybersecurity laws, measures that can be taken to protect personal data. Though some researchers have emphasized raising awareness, everyone has overlooked the importance of making aware of cybersecurity.

To fight the cybersecurity threat Bangladesh gov has declared a national cybersecurity strategy in 2014 [18]. In this strategy Bangladesh gov. has emphasized legal measures, creating national security council and framework, securing gov. infrastructure, sharing information and knowledge between gov. and private organization, national awareness program, and adding awareness to the national education. Though the gov. has declared the strategy in most of the cases gov. has failed to establish these strategies. Some seminars under the national awareness program currently have only been taken place on a limited scale such as some gov. organizations and public universities with very small numbers of participants. No tv program or symposium has not been telecasted from the gov. side to increase the awareness of mass people. Bangladesh gov. has included a subject to the national curriculum named ICT but there are very limited information and knowledge about the current cyber threats and vulnerabilities seen in Bangladesh and is not enough to teach the students about the safety and how-to response in case of exposure.

2.6 Problem Statement

The numbers of internet users have been increased over the years and cyber-attacks also have increased. The internet users are mostly not aware or educated in terms of information security. Because of their unawareness often they are unable to understand the threats of unauthorized access, result of the negligence and misuse of computer information technology, and many more issues. Loss of evidence lengthens the jurisdiction process and insufficient number of experts in the related field prevents the proper punishment of the criminals. The current strategies to fight the cyber threats in Bangladesh have not met the requirement of the current information security situation in Bangladesh. The government mostly focused on organizational level cyber threats and most of the strategy has been taken considering gov. and private organizational security threat. The importance of increasing information security among the mass people has been overlooked. Though gov. is working on increasing awareness no proper plan has been established. The education has been included in the national curriculum by Bangladesh gov. is failing to provide definite knowledge about current and future cyber threats in Bangladesh. It mostly discusses the general concept of computer, internet, and communication but not focusing on the knowledge about cybersecurity which can increase awareness. Some key problems faced by Bangladesh are described below:

- Increasing number of Cyberattacks in public and private sectors.
- Lack of knowledge about cyber safety.
- Uses of unauthorized/pirated software in daily life [19].
- Insufficient knowledge about existing law.
- Pornography.
- Cyberbullying.
- Identity theft.
- Scamming.
- Cyber violence against women. [19]

A proper education about cyber and information security and safety can be an effective solution to fight these current problems. Including such education in secondary school lever along with the current education will be effective and build a conscious generation for the future.

3. Methodology

The proposal of including courses in cybersecurity at the secondary education level requires a rigorous survey that should imply the success of the hypotheses to some extent. Two types of the survey have been conducted to find out current situation Cyber Security among the Bangladeshi people. And another one was an experiment survey which was required to justify the proposal of inclusion of Cyber Security education in Secondary school level.

The offline survey was done with a view to extracting the opinion from the guardians of minors. The online survey consists of people from all walks of life who have internet access.

3.1 Research Design

A qualitative research method was used in this thesis in order to find out the complete picture of the research group. In qualitative research, a semi-structured manner was followed. The main objective of qualitative research is to find out accurate and detailed information from the participants. Considering all aspects, a qualitative research was the most appropriate research method for this thesis. detailed information from the participants. Considering all aspects, a qualitative research was the most appropriate research method for this thesis. However, it is important to mention that the effectiveness of this method mostly varies on the researcher’s expertise. Opinion and biasedness of participants can manipulate the outcome of the findings.

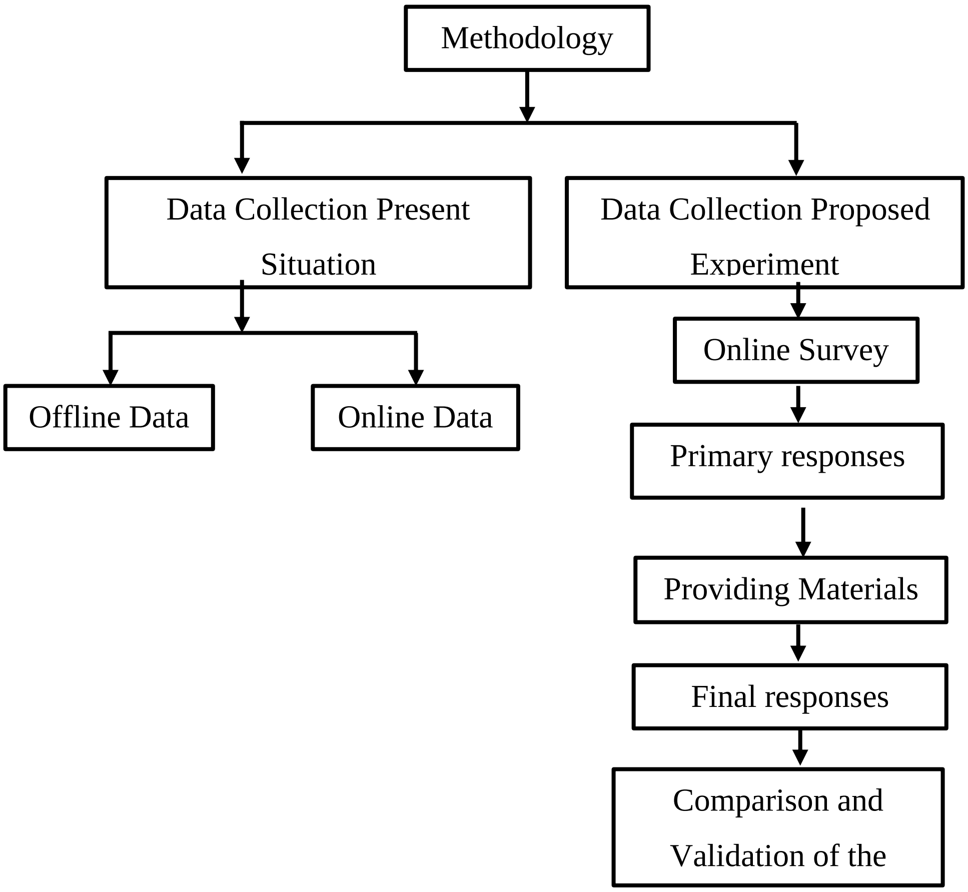

Methodology
Data Collection Present Situation
Data Collection Proposed Experiment
Offline Data
Online Data
Online Survey
Primary responses
Providing Materials
Final responses
Comparison and Validation of the

Figure 5. Research Design.

3.2 Data Collection for Present Situation

The survey was done both electronically and physically. Two surveys were done where the number of participants was 50 and 208. During offline data collection, people were surveyed from several locations spanning over the Sylhet and Dhaka division of Bangladesh. The offline survey was mainly done on the parents who have a school going child and have access to the internet regardless through their own device or their parents (attached in appendix 3). Purpose of collecting data from the parents of minors was to identify whether they are able to provide basic information about safe usage of the internet and electronic devices.

The online survey was done with the help of Google Form. Several questions regarding cybersecurity and the survey taker’s gender, age, and education level were asked (attached in appendix 2). The participants were asked to fill up a form electronically and provide their opinion on how the cybersecurity course will affect their view on internet security.

3.3 Data Collection for Proposal Experimentation

This experiment survey was conducted to identify the effectiveness of inclusion of information security at the Secondary School level. A group of 56 students below 18years old has participated in the survey were given some scenario based on real cases and their responses were listed (attached in appendix 4). After that, a material was given which was created based on a textbook for secondary education on Cyber Safety Manual by the Indian education board [20] (attached in appendix 5). Any Cyber Security or Cyber Safety-related book is not available in Bengali to which could be used for Bangladeshi students as a study material. This book was written for secondary school students of India who are the focused group this thesis as well. |After providing the materials, the same questions were given to them to see if proper information has a positive impact on their responses.

4. Result Analysis

Data collected from the participants has been analyzed to find out the overall situation of Cyber Security in Bangladesh. Different types of questions were asked based on the usage pattern of the user, available resources, knowledge, and demographic information. Collected data was analyzed for the present situation and proposal experiment separately.

4.1 Result Analysis for Present Situation

The present situation of result analysis was based on offline and online data. Offline data represents the condition of guardians/parents of minors in Bangladesh where online data mostly represent overall scenarios of youths of Bangladesh.

4.1.1 Offline Data

1. The parents were asked about the number of children they have in their family. The response was following

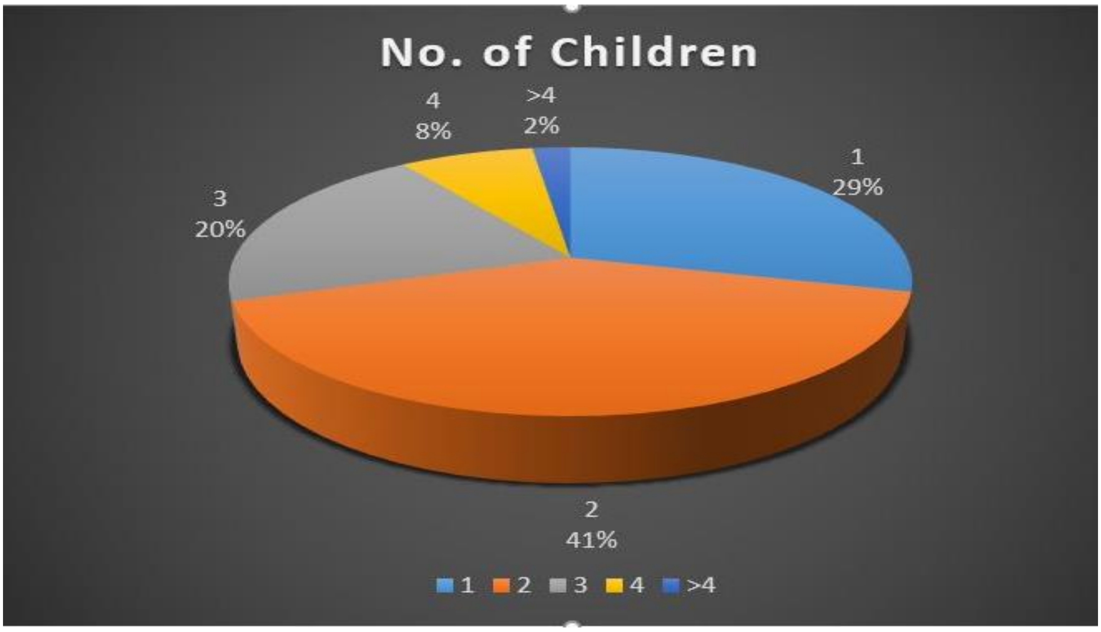


Figure 6. Pie diagram of number of children in a family.

In this figure, it can be seen that almost half of the parents have a family consisting of two children, whereas the other half is consisting of 1 and 3 children. Very few families have 4 or more children according to the survey data.

2. The education level of the guardians are as follows.

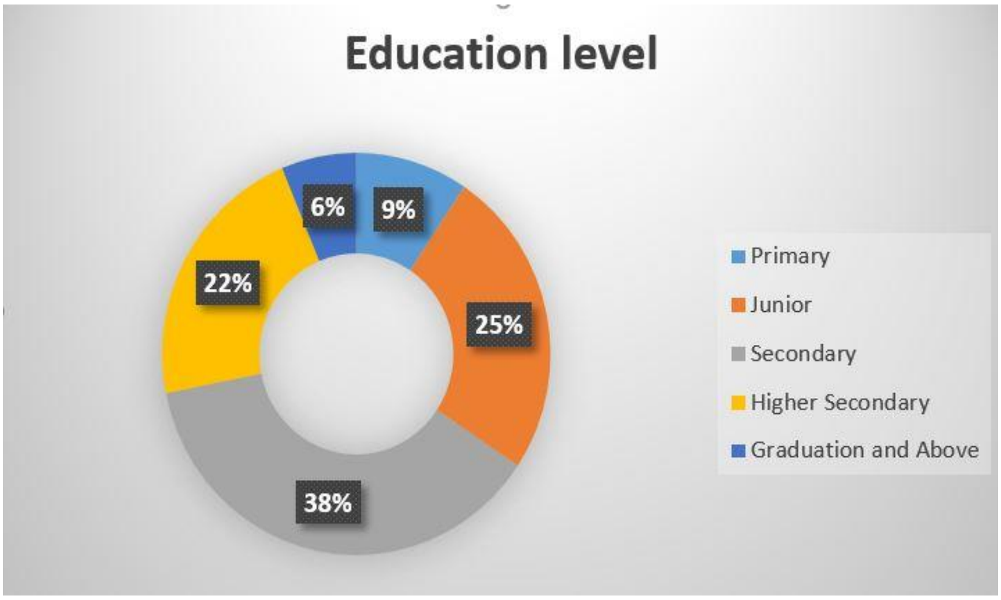


Figure 7. Doughnut chart education Level of parents.

This figure is about the education level of the parent. We see that most of them have completed at least junior level education which is up to standard 8 in Bangladesh. 22% of the participants have completed up to higher secondary and the number above the graduation level declines heavily after the higher secondary. This is important info on the mentality of the parents on cybersecurity. Most of the parents who have achieved education up to graduation tend not to overlook the potential threat of cyberbullying hence creating a significantly amicable environment for the children with mobile devices. On the other hand, those who have finished only up to higher secondary and did not have any education or knowledge on internet security tend to overlook the posed threat by cyberbullying.

3. In the survey, the parents were asked whether their children had a device of their own or used their parents'. The response depicted the followings-

Most of the parents said their children have a device of their own (63 of them) and only 23 said the children use their parent's device to go to the internet.

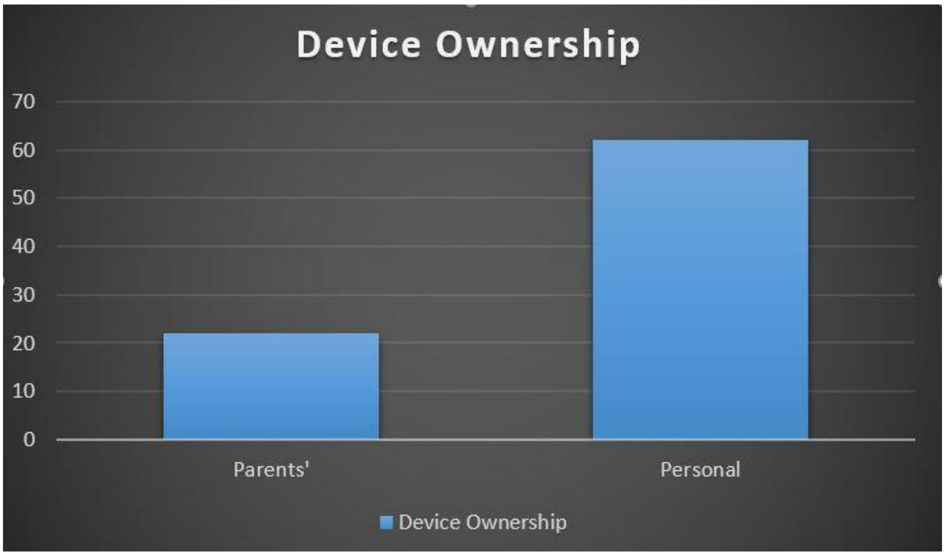


Figure 8. Device ownership status chart.

Most of the parents said their children have a device of their own (63 of them) and only 23 said the children use their parent’s device to go to the internet.

4. The parents/s were asked what their children say when asked about the purpose of using the internet. There were only two options to choose between and the parents responded accordingly.

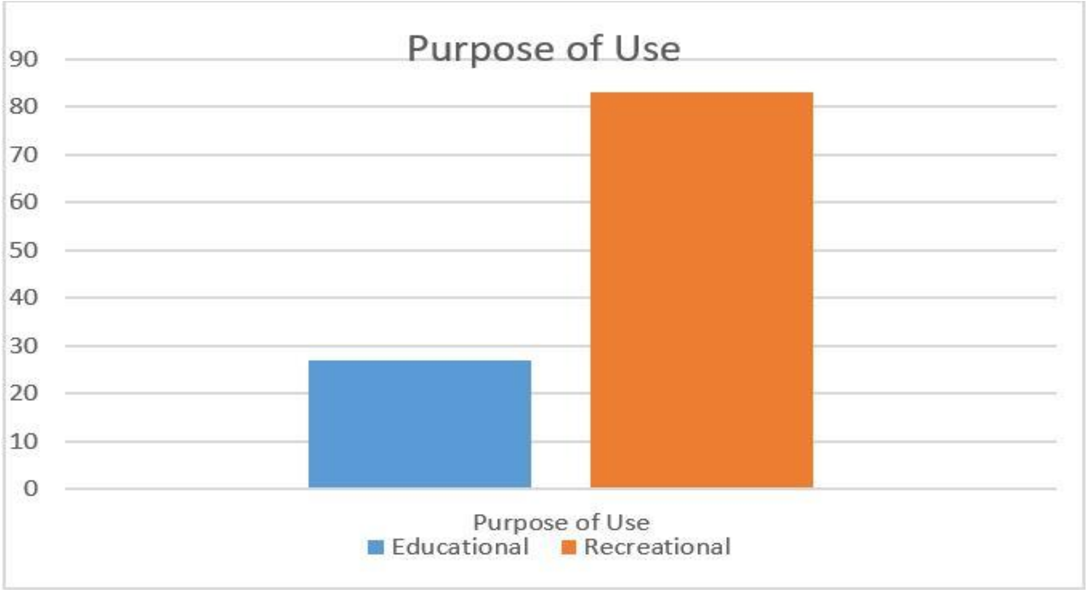


Figure 9. Purpose of using device chart.

In this figure, we see that 83% of the children use the internet for recreational purposes where only 27% of them uses for both educational and recreational purpose, as reported by their parents. That number alone is alarming for the community since excessive use of the internet only for recreation poses a decent threat to the children being exposed to cybercrimes like child pornography and phishing. Data theft and misuse of user data also pose a significant threat, not to mention the impact these contents have on a child’s mind.

5. Total time spent in a day on the internet (in hours) was also included in the survey. The data were as follows-

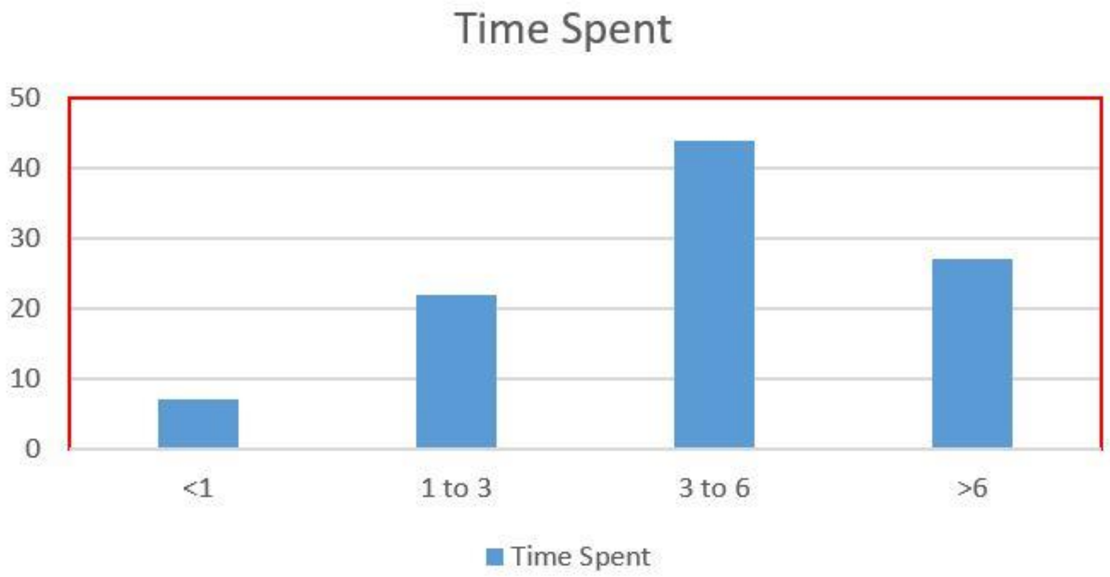


Figure 10. Time spent in a day for internet (hours) chart.

We know that most cellphones have a feature called digital wellbeing which reports how long the phone has been used each day. Although most of the parents are unaware of the existence of this feature, they reported that their children use cellphones for 3 to more than 6 hours per day. Almost 68% of them uses cellphone for more than 3 hours a day and the others said the duration spans from 1 to 3 hours daily

6. Parents were asked if they checked their children's device history. There was a mixed response to that question which is depicted by the following.

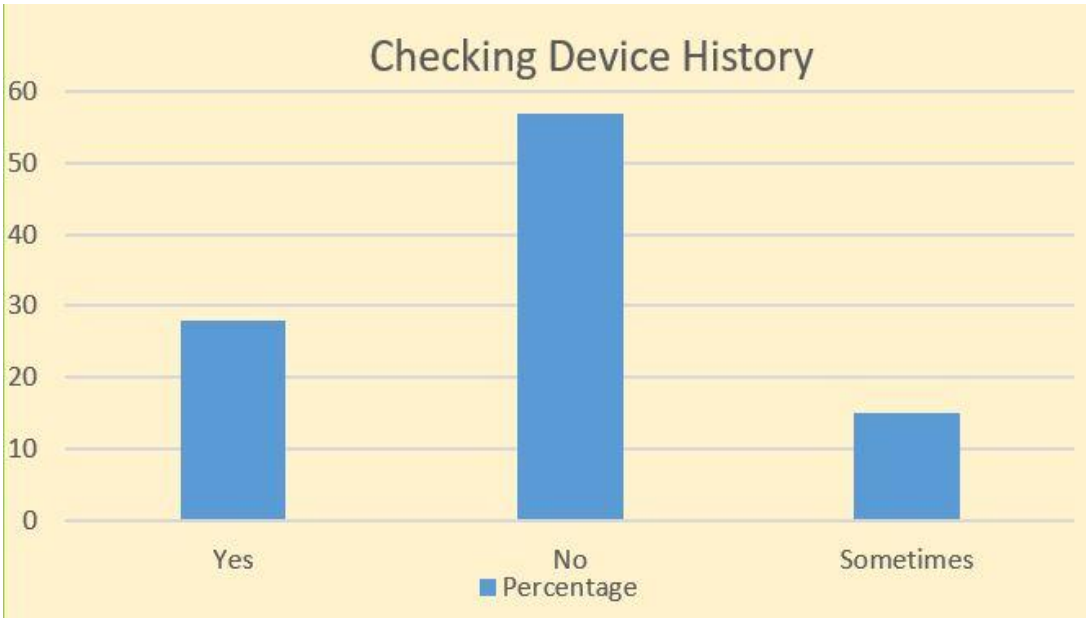


Figure 11. Device history checking chart.

During these periods most of the parents do not check the device history of their children, hence being clueless about what their children are up to. In this figure, we can see that, 28 of the participants said they checked the device history regularly and the rest of them said they check it sometimes but not regularly.

7. The parents were asked whether they knew about parental control or not. Results are-

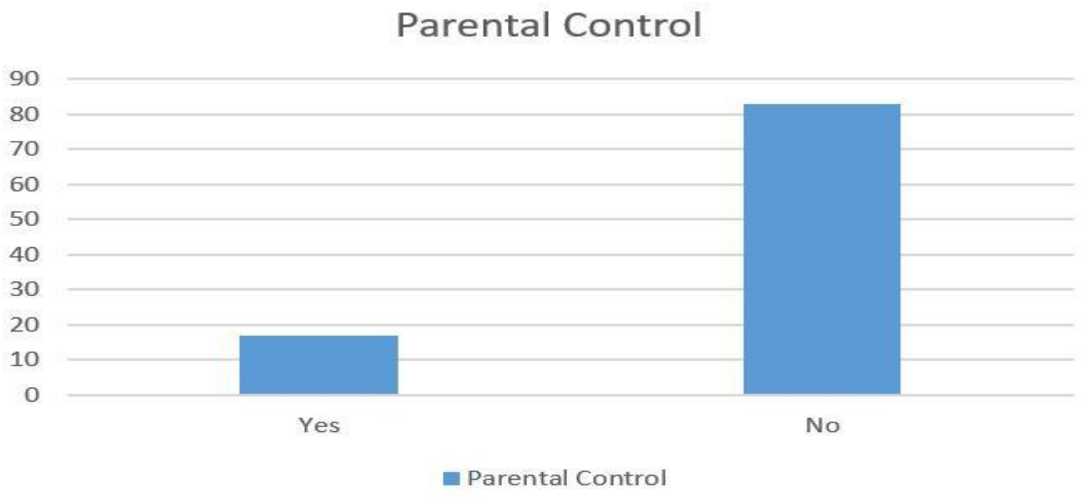


Figure 12. Parental control knowledge chart.

In this figure, we can see that most of the parents (83 of them) did not have any idea about parental control which is very important for cybersecurity assurance.

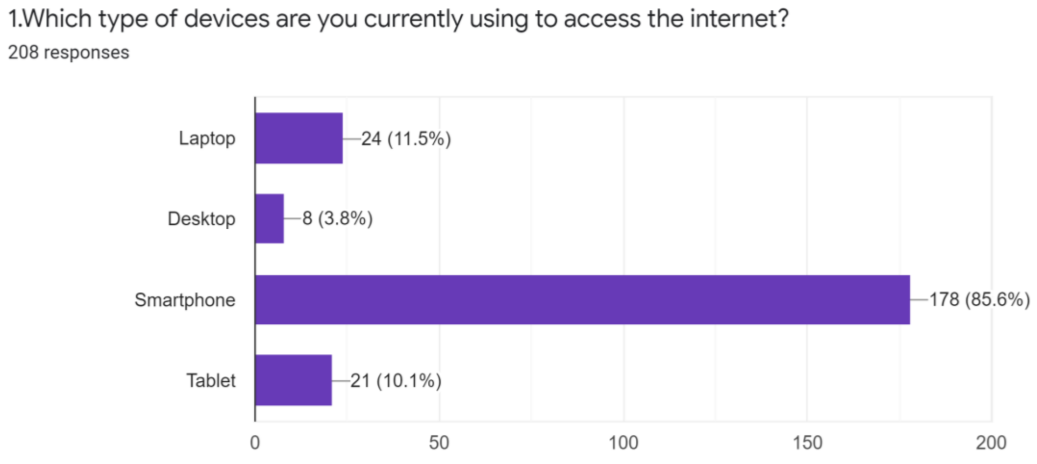
Finally, the survey demanded to convey their opinion on improving the current situation of cybersecurity in Bangladesh. Most of them emphasized the following steps

- Including a cybersecurity course in primary-junior level
- Airing TV program for ensuring awareness among children
- Discussion between the children and parents

4.1.2 Online Data

An online survey was carried out with the help of google form. The survey was about the internet and cybercrimes. The link was circulated throughout social media and several age groups. The responses were recorded and analyzed using the same tool. There were 208 participants. The survey was conducted targeting the youth, but there was no specific age restriction.

After that, we conducted another survey on the internet & cybercrimes based on the person’s view. The following responses were recorded during that survey.



1.Which type of devices are you currently using to access the internet?

208 responses

Figure 13. Responses for device types.

In this figure, we see that almost 85.6% of people use a smartphone to access the internet. 11.5% uses laptop, 3.8% uses desktops and 10.1% people uses a tablet to do it.

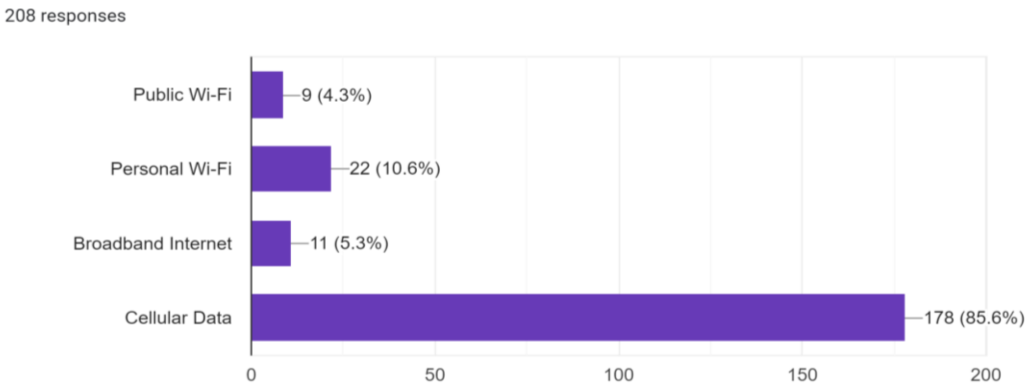


Figure 14. Responses for internet access types.

In this figure, we see that 85.6% of people cellular data to access the internet. 4.3% use public Wi-Fi, 10.6% uses personal Wi-Fi and 5.3% uses broadband internet.

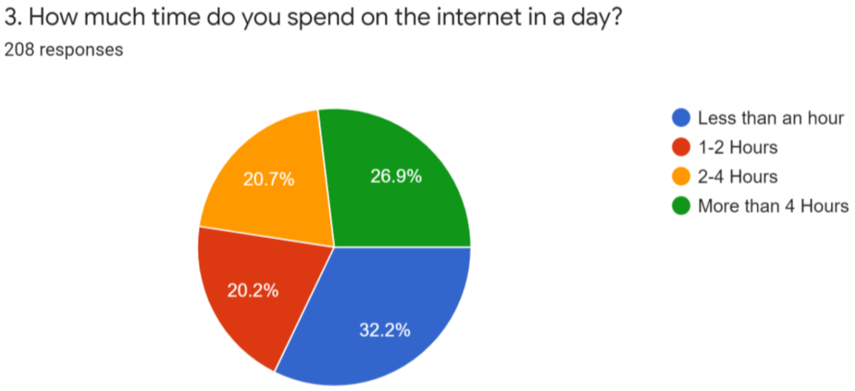


Figure 15. Time period responses.

In this figure, we can see that 32.2% uses less than an hour, 26.9% uses more than 4 hours, 20.7% uses 2-4 hours and 20.2% uses 1-2 hour in the world of internet.

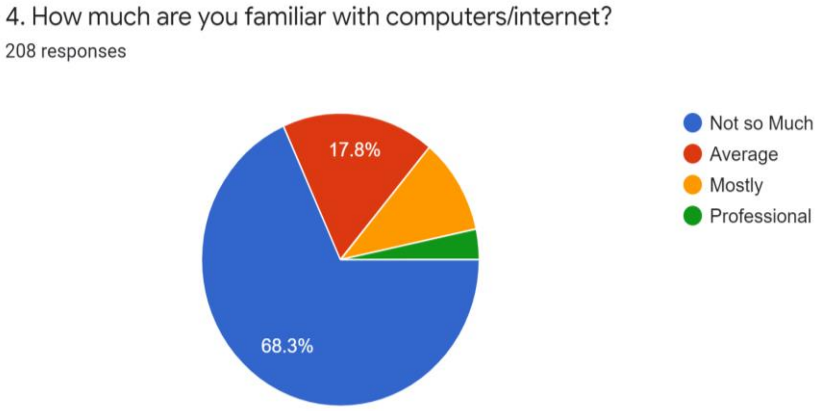


Figure 16. IT knowledge-based responses.

In this figure, we can see that almost 68.3% of people are not so familiar with computers, 17.8% are average and the rest are mostly and some of them are professional

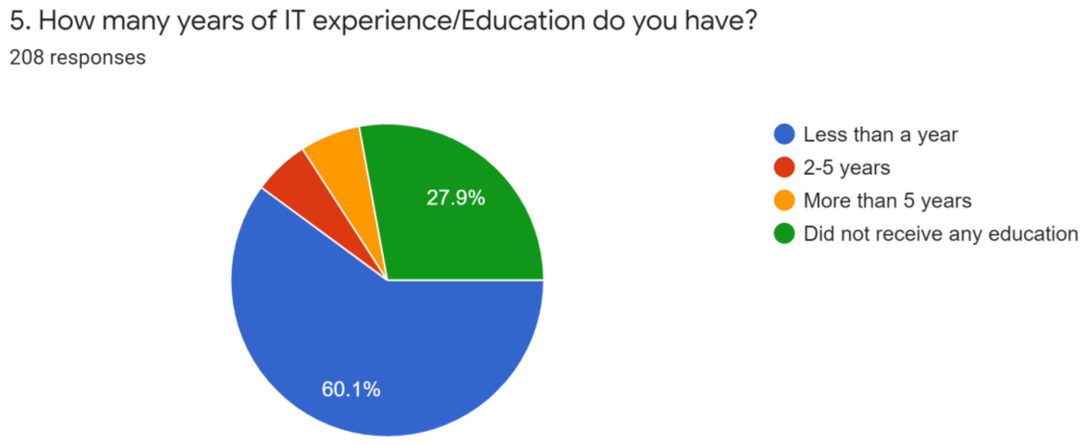


Figure 17. IT Experience based responses.

In this figure, we can see that 60% of people have lower IT experience for less than a year, and 27.9% of people did not receive any education about it. The rest had experienced more than 2 years.

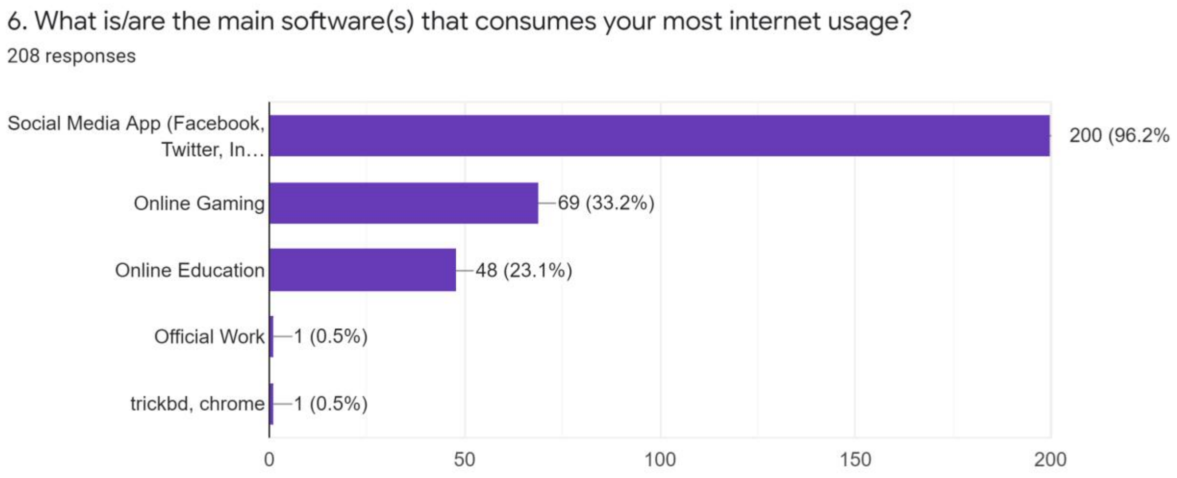


Figure 18. Software consumption-based responses.

In this figure, we can see that almost 96.2% of people consumed their internet usage for social media apps like Facebook, Twitter, Instagram, What’s app, etc. 33.2% used it for online gaming and 23.1% used it for online education.

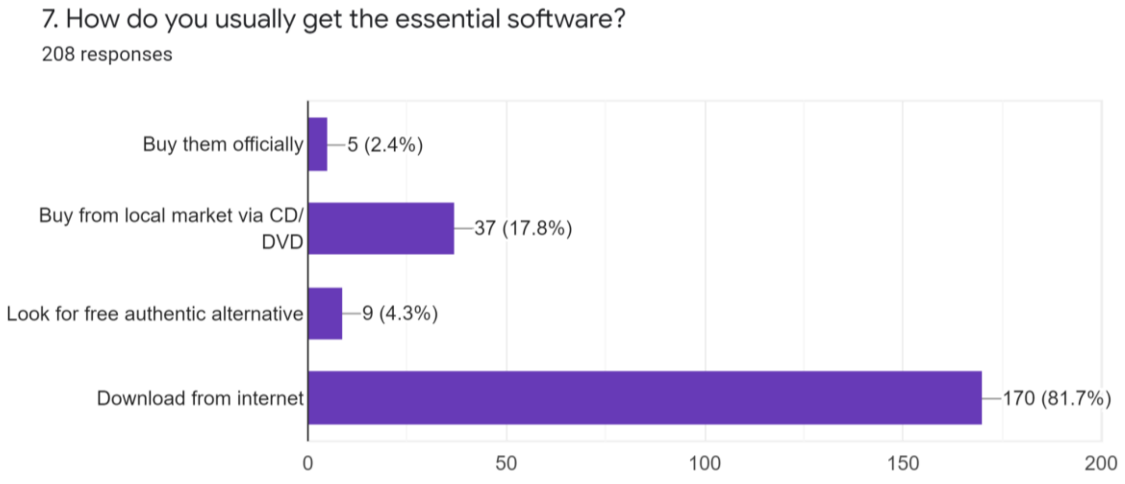


Figure 19. Way of getting the Software based responses.

In this figure, we can see that only 2.4% of people thought of buying software officially and 4.3% thought to get an authentic alternative free version. 17.8% of people bought from a local market and 81.7% people thought to download from the internet.

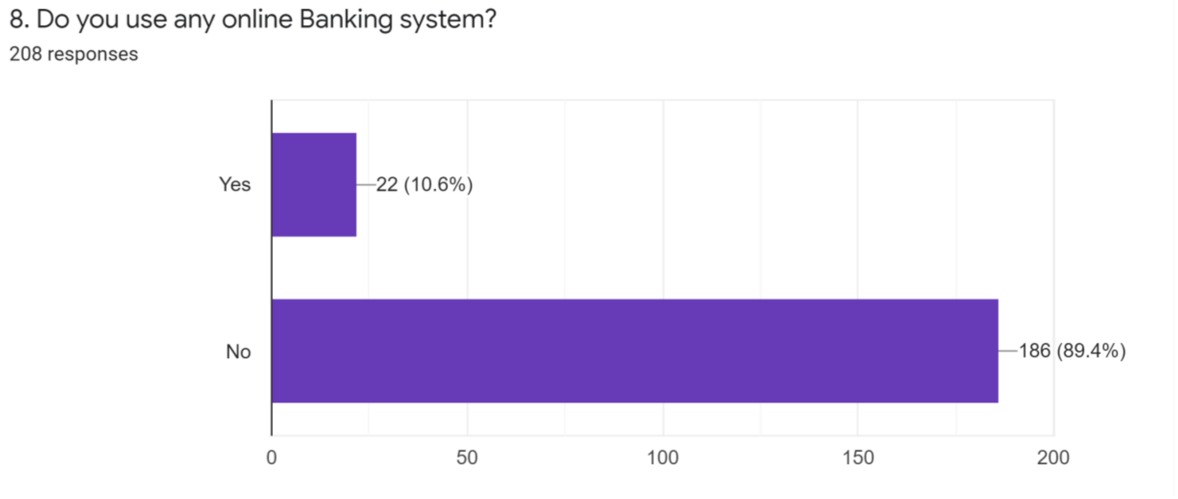
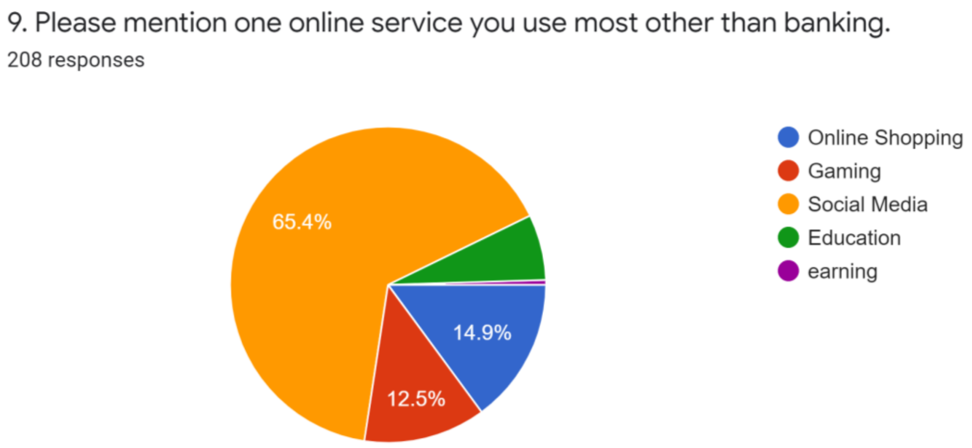


Figure 20. Online banking system-based responses.

In this figure, we can see that 89.4% of people used the online banking system. So, they are vulnerable to financial cybercrimes.

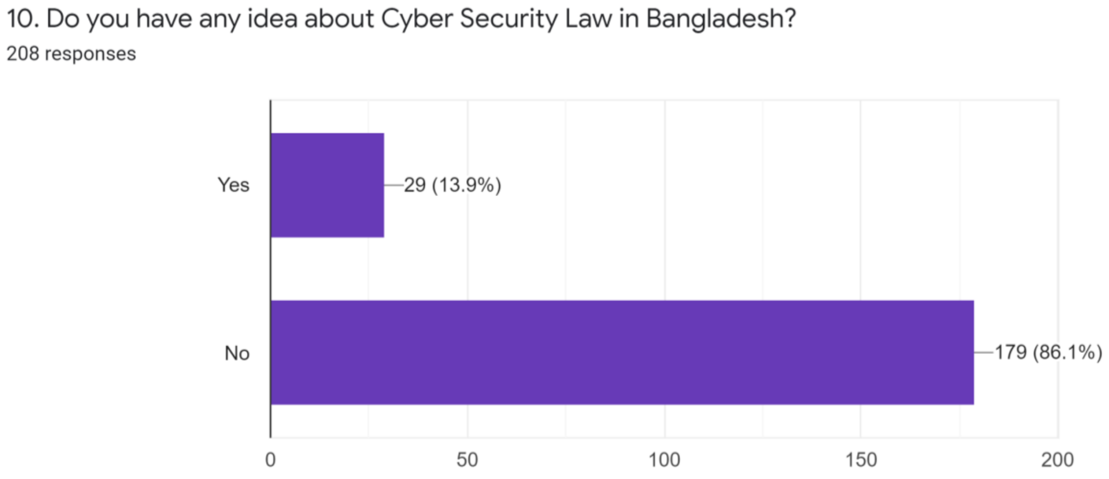


9. Please mention one online service you use most other than banking.

208 responses

Figure 21. Other online services-based responses.

In this figure, we can see that other than the online banking system 65.4% of people used social media, and the rest like 12.5% & 14.9% used gaming & online shopping. The rest used it for educational purposes and as an earning medium.



10. Do you have any idea about Cyber Security Law in Bangladesh?

208 responses

Figure 22. Acknowledgment of cybersecurity-based responses.

In this figure, we can see that 86.1% of people had no idea about cybersecurity law in Bangladesh and 13.9% only knew about that law

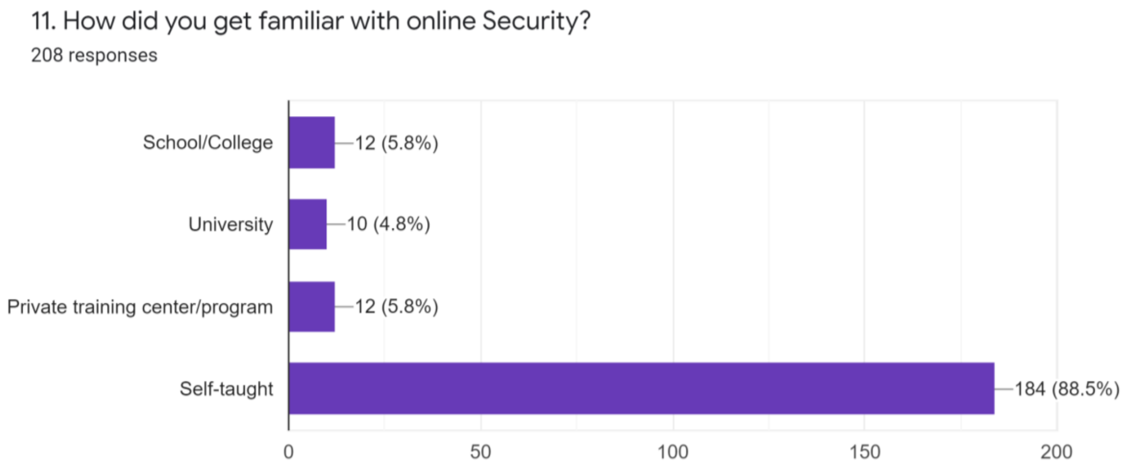


Figure 23. Way of familiarization to online security-based responses.

In this figure, we can see that 88.5% of people were self-taught about cybersecurity. Only 5.8% learned it in school, 4.8% in college, and 5.8% learned that via training center.

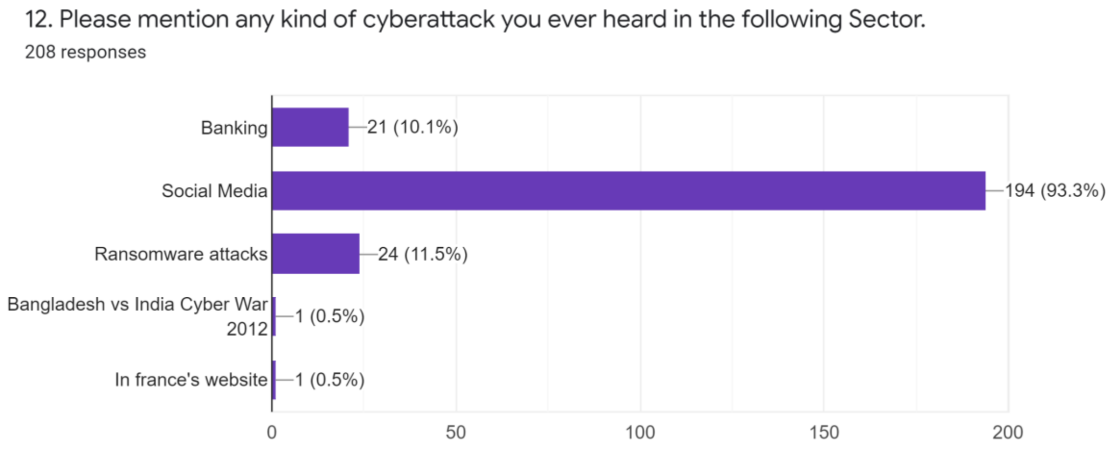


Figure 24. Acknowledgement of cybersecurity-based responses.

In this figure, we can see that 93.3% of people heard about social media-based cybercrimes. They did not have any idea about other cybercrimes. Only 10.1% heard about banking and 11.5% knew about ransomware attacks.

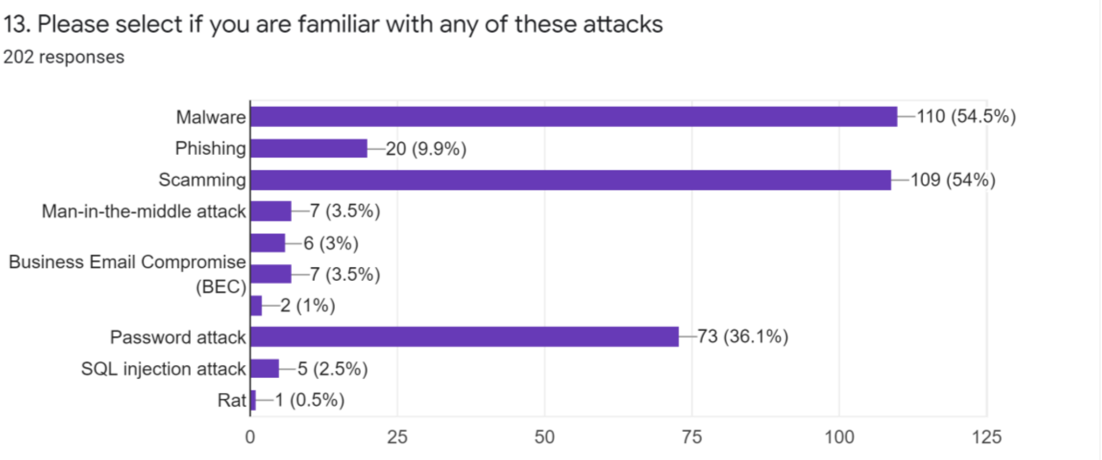


Figure 25. Example of cyberattacks based responses.

In this figure, we can see that almost half of the participants only knew some of the common cyberattacks but most of the cyberattacks were unknown to them.

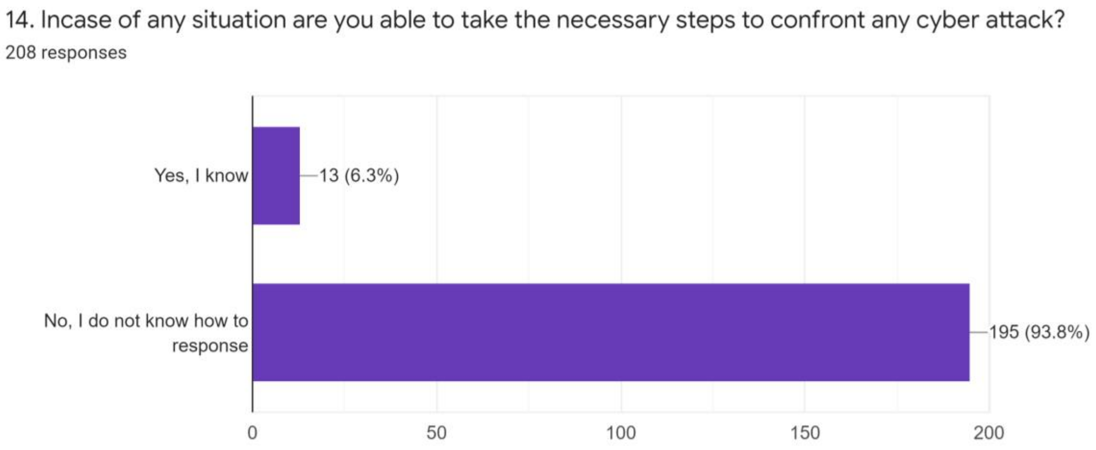


Figure 26. Knowledge about confronting cybercrimes-based responses.

In this figure, we can see that almost 93.8% of people did not know how to respond if they confront any cyberattacks. Only 6.3% of people knew the way of confronting it.

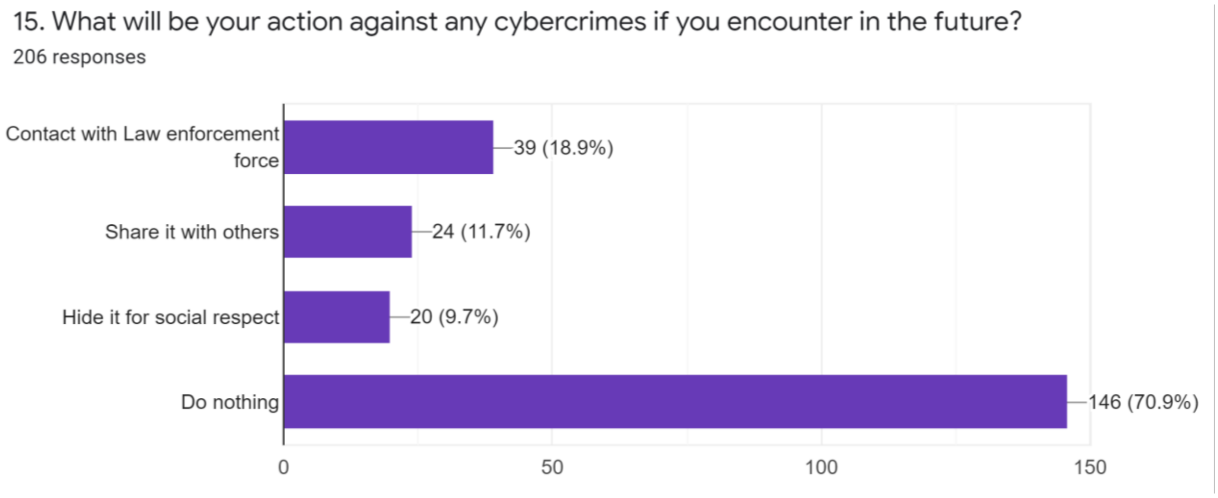


Figure 27. Future actions against cyberattacks based responses.

In this figure, we can see that almost 71% of people did not think to do something when they encounter any cybercrimes in the future. 18.9% responded to contact with law enforcement force, 11.7% thought about sharing it with others and 9.7% wanted to hide it for social respect.

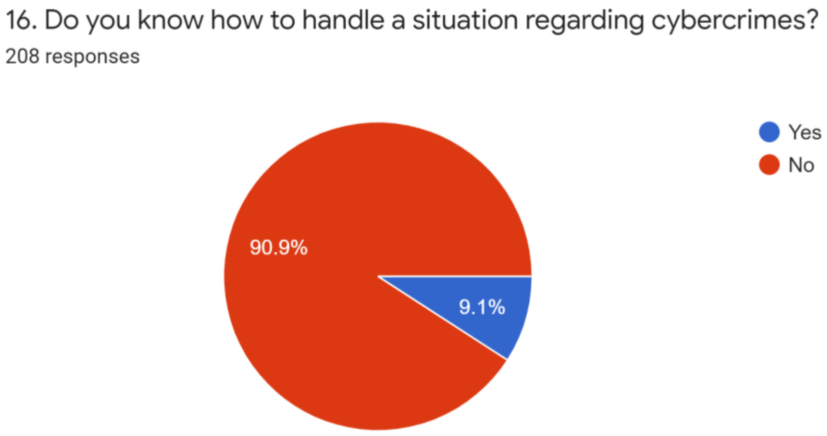


Figure 28. Knowledge of handling cyberattacks based responses.

Almost 90% of people did not know how to handle the situation regarding cybercrimes as it could be with anyone and if they acknowledged it.

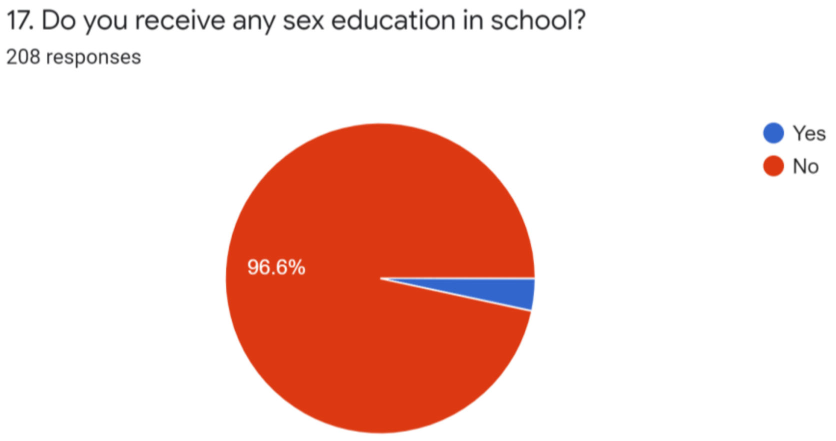


Figure 29. Sexual education-based responses.

Child pornography and adult website have a bad impact on children. So, they must get proper sex education. But unfortunately, 96.6% responded that they didn't receive any sex education in school.

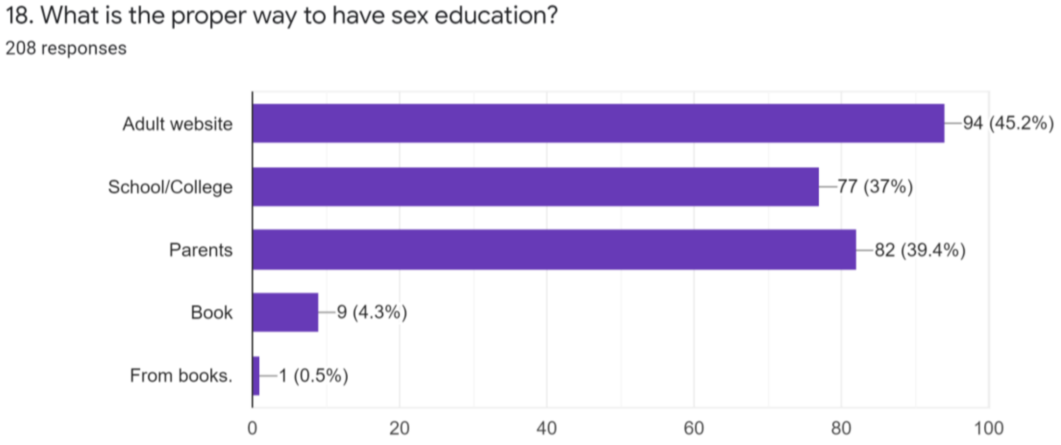


Figure 30. Way of getting Sexual education-based responses.

In this figure, we can see that 45.2% of people think adult website is a proper way to get sex education which is very alarming. But 37% of people thought about institutions and 39.4% thought for parents.

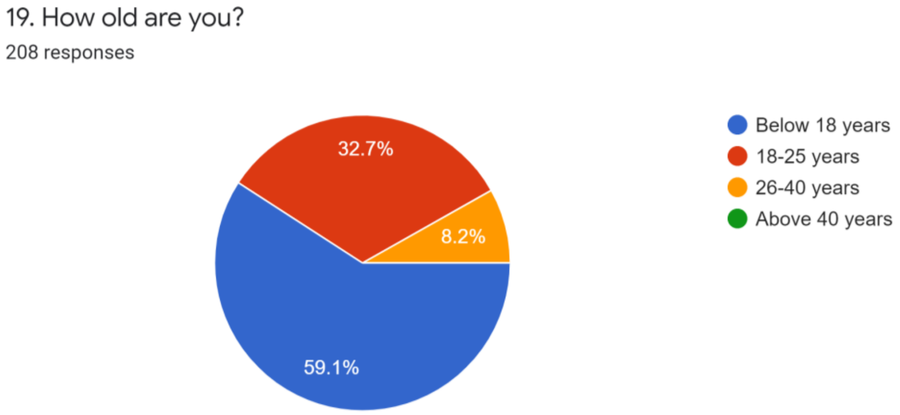


Figure 31. Age based responses.

In this figure we can see that almost 200 participants the most of them were between the age group of below 25 years, almost 92 percent of them said they were within that age of puberty and adulthood. 59 percent of the survey takers were under 18 years and hence this survey data will show how the young adults of the country are vulnerable to the internet world.

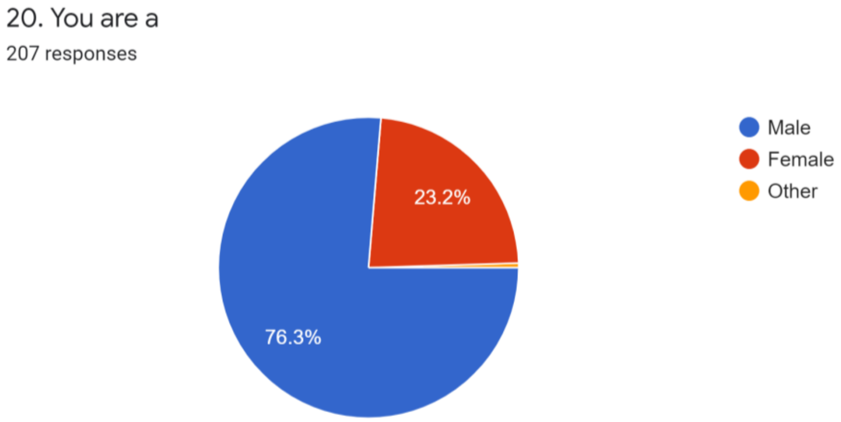


Figure 32. Gender based responses.

In our survey, there were 76.3% male participants and 23.2% female participants. That’s because, in Bangladesh, most of the boys get their device before any girls of the same age. The parents are more careful about their girl child than the boy child.

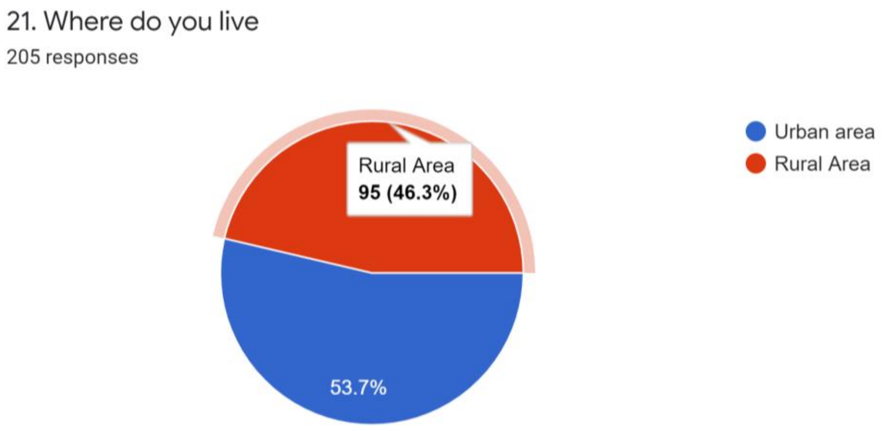


Figure 33. Area based responses.

Most of the participants were from urban areas (53.7%) and 46.3% of people were from rural areas.

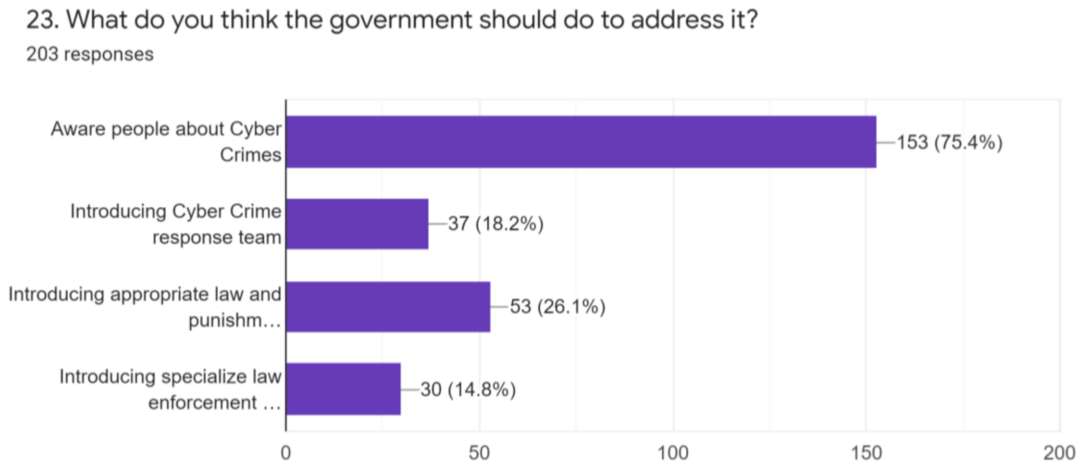
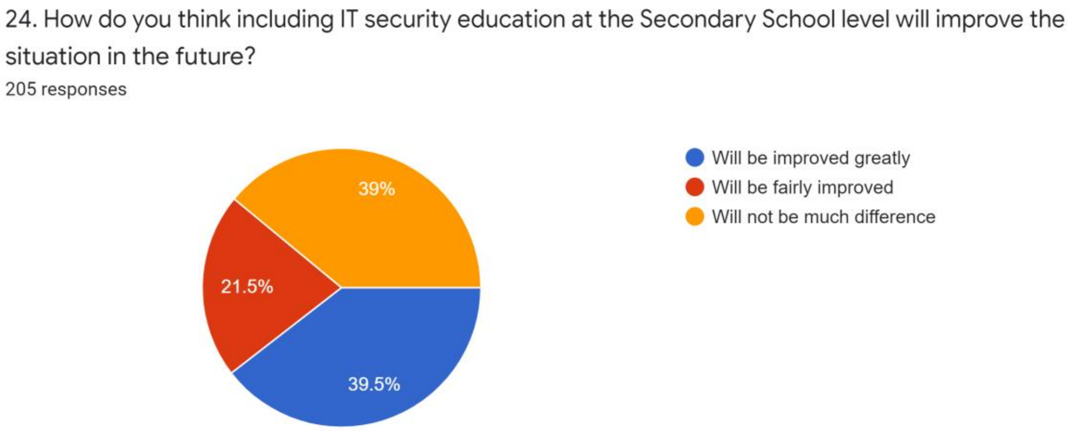


Figure 34. Suggestions towards government-based responses.

The above figure indicated the people’s suggestion about cybercrimes towards the government. 75.4% of people responded to aware people about cybercrimes, 18.2% proposed to introduce CERT team, 26.1% people thought about introducing law and punishment, and 14.8% people suggested to implement special force.



24. How do you think including IT security education at the Secondary School level will improve the situation in the future?

205 responses

Figure 35. Including cybersecurity in education-based responses.

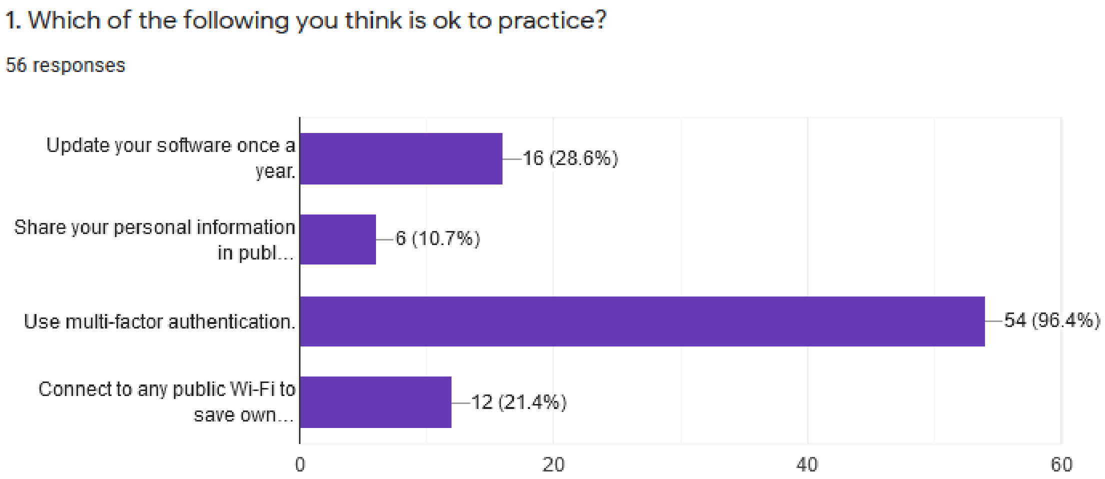
In this figure, we can see that 39.5% of participants thought that inclusion of cybersecurity in the secondary school level will improve the situation greatly, 21.5% responded positively and 39% people did not think that will make some differences.

After a productive survey on cybersecurity and cybercrime on different age groups, we can say that people need to know a lot about those topics. They have less knowledge about it. We also provide the young group some materials based on cybersecurity to see their responses. This material consists of detailed knowledge about some important points[21]. Those are given below.

- Basic knowledge about cybercrimes
- Knowledge about the medium of cybercrimes on different platforms
- Protection knowledge from web-based and system-based attacks
- Knowledge about cybersecurity law and how to confront it
- Knowledge about used software vulnerabilities
- Knowledge about choosing software consciously, wisely to avoid malware-prone ones

4.2 Proposal Experiment

In this experiment survey, a group of 56 students aged below 18 participated. Their responses were judged based on the real scenario in the quiz from where they were not given any feedback instantly. It was not possible for the participant to know if their responses were appropriate to the respective situation instantly. The responses of participants are discussed below-

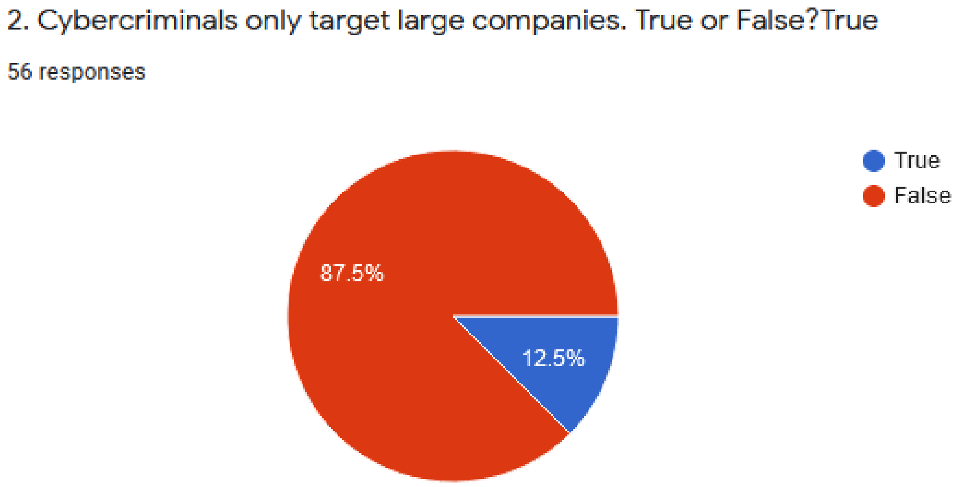


1. Which of the following you think is ok to practice?

56 responses

Figure 36. Primary cautions responses after study.

On the first figure, we saw that most people thought updating software was more important than having authentication in a multiple-way but after the study of the materials, 70% of the participants agreed that multifactor authentication is more important than an update.

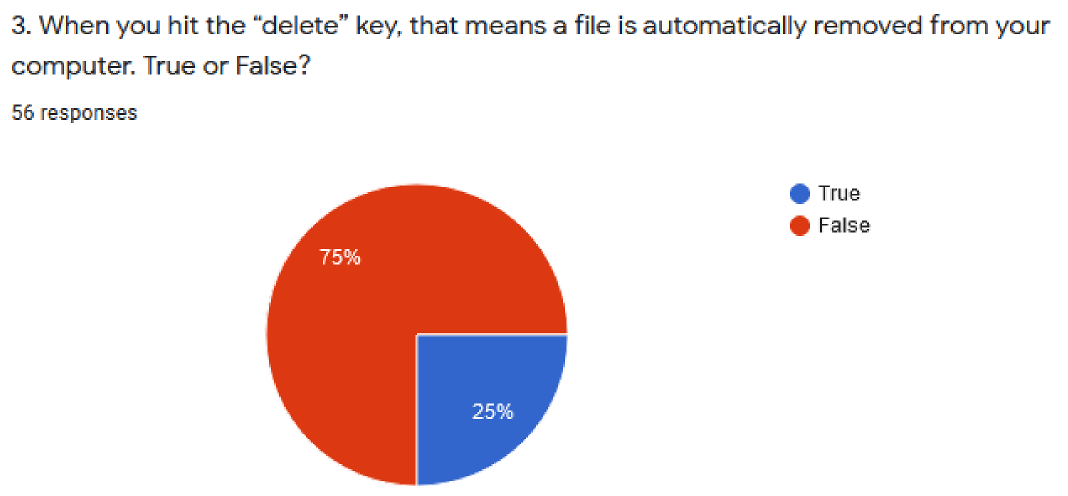


2. Cybercriminals only target large companies. True or False?True

56 responses

Figure 37. Target area responses after study.

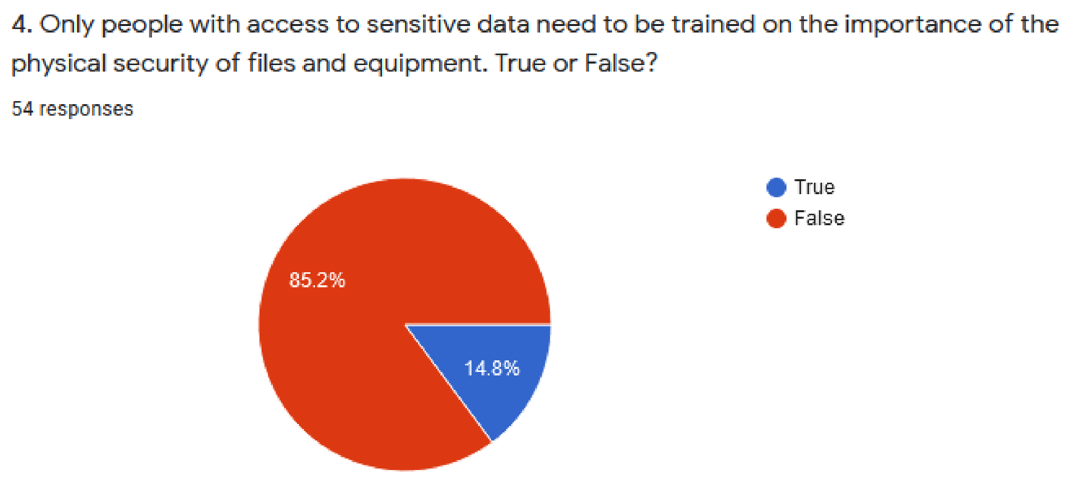
In this figure, we can see that before studying the materials most people thought that cybercrime could only happen to large companies but after studying almost 70% people changed their minds.


3. When you hit the “delete” key, that means a file is automatically removed from your computer. True or False?

56 responses

Figure 38. Deleting knowledge responses after study.

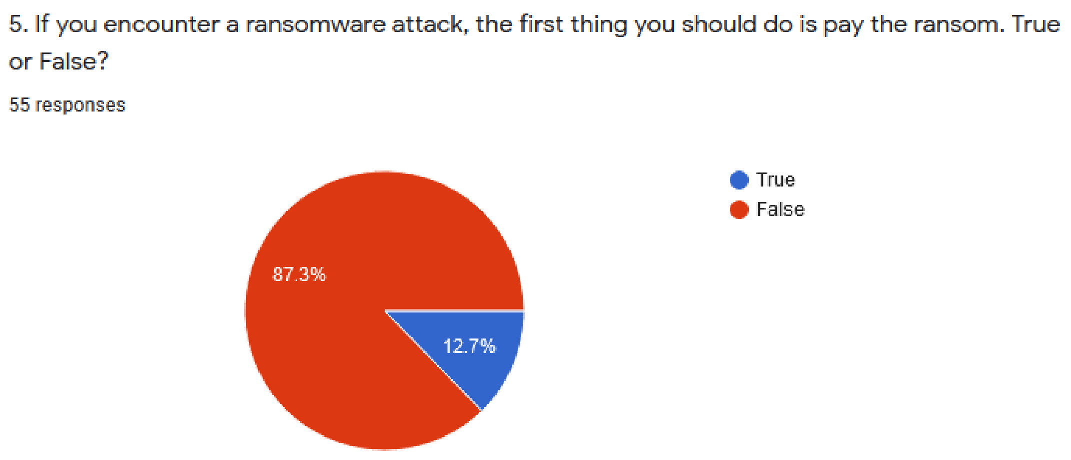
Almost 80% of people thought that ‘delete’ is the key to remove a file from your computer permanently but in this diagram, we can see that later almost 55% of people realized that is not true. They changed their opinion.


4. Only people with access to sensitive data need to be trained on the importance of the physical security of files and equipment. True or False?

54 responses

Figure 39. Requirement of IT based knowledge responses after study.

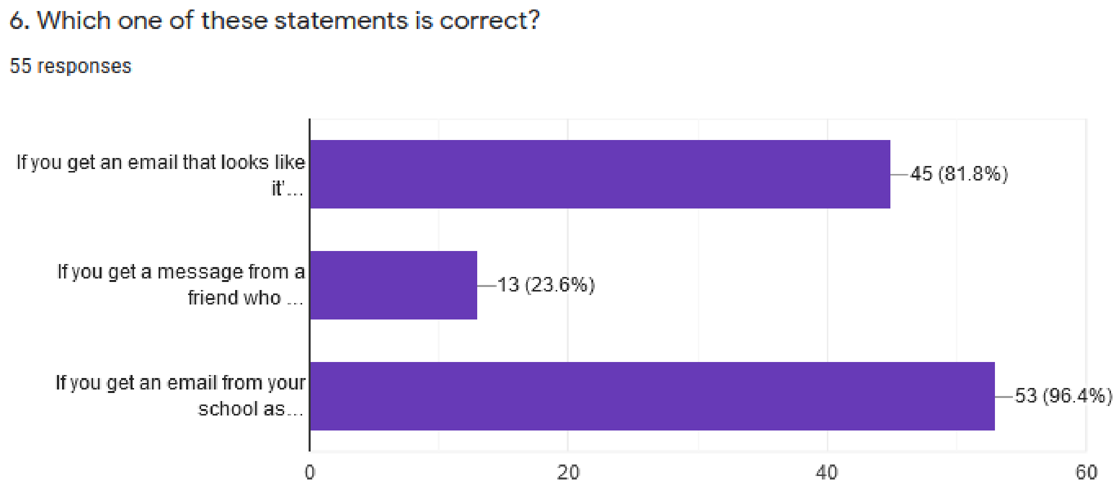
Around 82% of people thought that cybersecurity was not important for all, it was only for those who had access to some sensitive data. In the figure, we can see that after studying almost 67% of people improved their opinion.


5. If you encounter a ransomware attack, the first thing you should do is pay the ransom. True or False?

55 responses

Figure 40. Checking about first steps knowledge responses after study.

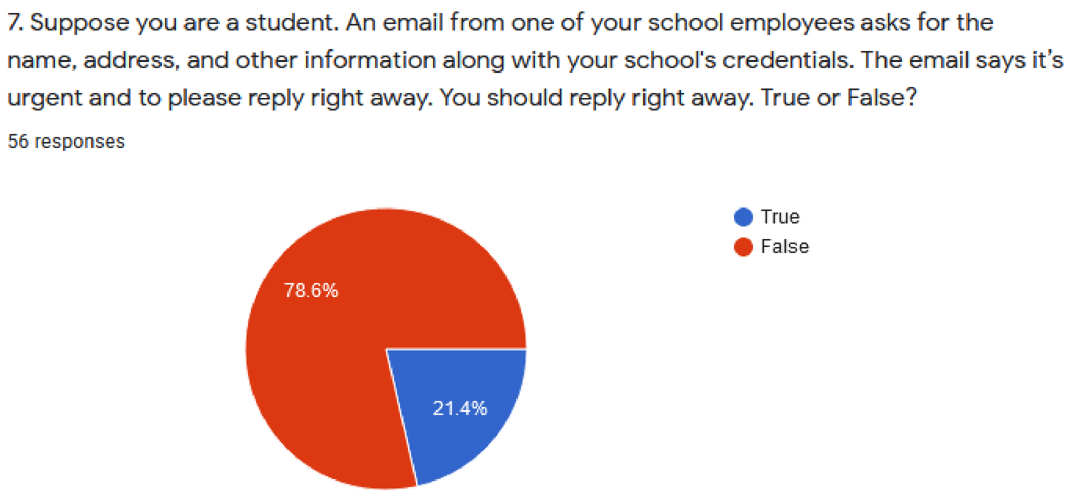
76% thought paying ransom was the right thing to do but, in the diagram, we can see that after the study 64% changed their option not to do that.


6. Which one of these statements is correct?

55 responses

Figure 41. Personal information protection-based responses after study.

76.8% of people thought that if there was a defender they can click on any link and download anything from the internet but in this figure, after the studying around 80% of people understand that was not safe, we also provide them an example situation where we could see that 53% people had successfully got the situation correctly.

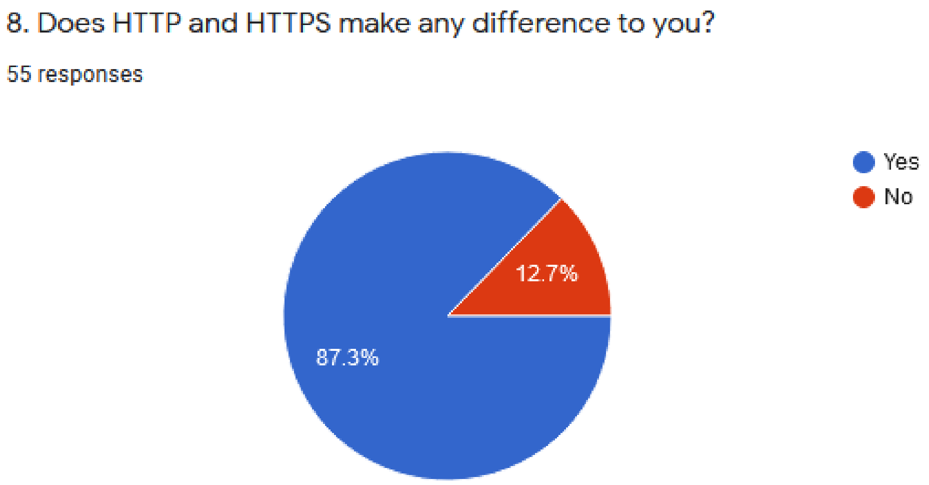


7. Suppose you are a student. An email from one of your school employees asks for the name, address, and other information along with your school's credentials. The email says it's urgent and to please reply right away. You should reply right away. True or False?

56 responses

Figure 42. Example based personal information protection responses after study.

There was an example regarding personal information and to provide it if it was sent from a trusted source and 76.8% of people agreed to provide the information without any authentication. But in this diagram, we can see that almost 55% of people changed their thought after the study material.

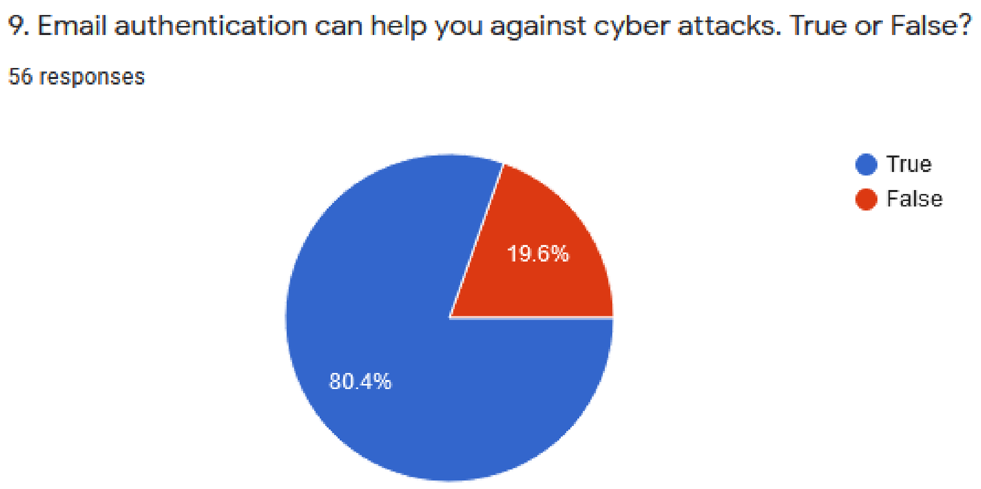


8. Does HTTP and HTTPS make any difference to you?

55 responses

Figure 43. Protected link-based responses after study.

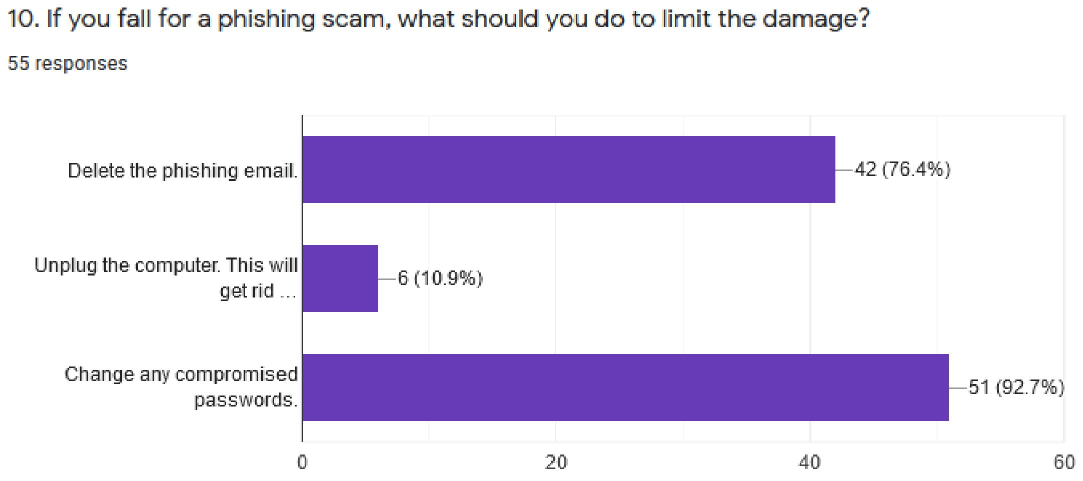
In this figure, we can see that almost 67% of people knew the difference between HTTP & HTTPS after studying the material.


9. Email authentication can help you against cyber attacks. True or False?

56 responses

Figure 44. Authenticating email responses after study.

In this figure, we can see the improvement in the email authentication knowledge of the participants. Almost 72.7% of people thought it correctly but after the study, we see the percentage rose to 80.4% which is a good improvement.


10. If you fall for a phishing scam, what should you do to limit the damage?

55 responses

Figure 45. Recovering steps-based responses after study.

87% & 66% of people thought that deleting phishing mail and unplugging devices world help to get rid of the situation. But in this figure, we can see that after the study almost 93% of people thought that changing a compromised password would be more effective. Almost 80% of people improved their knowledge and situation.

After considering those improvements, we can see that there is a huge difference on responses between the pre-material survey and post-material survey. In every question around 53% - 80% of people improved their knowledge, their thoughts. So, considering the improvement in age below 18 we can say that if cybersecurity or IT-based knowledge is included in our education system, it will make a huge impact in the future.

4.3 Future Scopes

There are some future scopes in this hypothesis. Those will be mentioned below for further research in the future.

- Although the dissertation proves the claim that the inclusion of a course in cybersecurity in the secondary or junior level will increase the chance of internet users being alert for the incoming cyber threats, it goes without saying that much work can be done to improve the outcome.
- While doing the survey, most of the survey takers were from the privileged group with an internet device and access to broadband internet. The range of survey takers can also be increased to get a vast idea of how the inclusion of a course would be beneficial for their digital wellbeing.
- More opinion from the policymakers can be added to ensure that they do think this inclusion to be a feasible option to educate the mass-people. The idea of a course inclusion in primary education can also be considered since day-by-day internet will be more accessible to people from all age groups.

5. Conclusion

In this thesis, the author tried to describe the present situation of cybercrime in the world and how Bangladesh is doing on that. It is also described as the categories of cyberattacks based on system, web, and users. The author classified the types of criminals in general. Also, describe the reasons behind cybercrimes. After that, the present situation in Bangladesh, and the cybersecurity law status in Bangladesh was discussed. The punishment of cybercrimes was described also in a nutshell.

Two types of the survey were conducted to prove the hypothesis. One is online based and the other one is offline survey for the parents. To conduct the offline survey, parents were given a paper-based questionnaire and acknowledged that most parents were not aware of cybercrime or cybersecurity. That survey proves that the parents in Bangladesh are not so concern about their children's safety about cybercrimes. In the online survey, the author took two of them to see the current situation of cybercrimes in Bangladesh and how the users were vulnerable to it. After taking that survey, it was confirmed that the people of Bangladesh do not know much about cybersecurity law in their country. So, to improve their opinion and thoughts, the author decided to conduct a survey on cybersecurity knowledge for the people who were young and under 18 years. For that, a survey was conducted first to see the current knowledge of that group and then the author provided them some materials to increase their knowledge about cybercrime and cybersecurity. So, after providing the materials, the author conducted the same survey again on them to see the improvement and surprisingly a convincing improvement was seen. That result proves that, if we add cybersecurity knowledge in the education system, it will help the people to improve their knowledge, their thoughts and in future maybe not to be a victim of a cybercrime. They can confront cyberattacks, handle their personal information wisely and we will see a bright generation who knew what to do and how to do if they will ever encounter any kind of cybercrimes. Thus, we will see a future with minimum loss caused by cybercrimes.

References

[1] “No Title.” https://www.javatpoint.com/cyber-security-introduction.

[2] M. M. Kamal, I. A. Chowdhury, N. Haque, M. I. Chowdhury, and M. N. Islam, “Nature of cyber crime and its impacts on young people: A case from Bangladesh,” Asian Soc. Sci., vol. 8, no. 15, pp. 171–183, 2012, doi: 10.5539/ass.v8n15p171.

[3] A. L. Wenden, “No Titl ปัจจัย พลาสติกชีวภาพ,” 1981. .

[4] K. Faisal, “Recent Trend and Issues of Cybercrime in Bangladesh-An Analytical Study,” 2018, no. July, 2016.

[5] N. Ahmed, U. Kulsum, M. I. Bin Azad, A. S. Z. Momtaz, M. E. Haque, and M. S. Rahman, “Cybersecurity awareness survey: An analysis from Bangladesh perspective,” in 5th IEEE Region 10 Humanitarian Technology Conference 2017, R10-HTC 2017, 2018, vol. 2018-Janua, no. December 2019, pp. 788–791, doi: 10.1109/R10-HTC.2017.8289074.

[6] M. Rahman, R. Akanda, M. Nadir, B. Ali, M. Parvez, and N. Islam, “A Survey on Cybercrimes Awareness Knowledge in Bangladesh,” no. February, pp. 0–7, 2019, doi: 10.13140/RG.2.2.30834.96968.

[7] “GOVERNMENT OF BANGLADESH INFORMATION SECURITY MANUAL | BGD e-GOV CIRT | Bangladesh e-Government Computer Incident Response Team.” [Online]. Available: https://www.cirt.gov.bd/government-of-bangladesh-information-security-manual/.

[8] "Open Web application security project Top 10 Web Application Security Risks" 2020, [Online]. Available: https://owasp.org/www-project-top-ten.

[9] A. R. M. Borhanuddin and B. Ramna, “Cybercrime and Bangladesh perspective,” 2006, pp. 1–15.

[10] F. A. Fabinu, T. O. Ogunleye, and A. T. Salau, “The Inclusion of Security Education in the Basic Education Curriculum : A Means for Preventing Child Abuse,” 2016, vol. 04, no. 02, pp. 71–77.

[11] “No Title.” https://www.ukessays.com/essays/information-technology/weakness-of-cyber-law-in-bangladesh-information-technology-essay.php.

[12] “No Title,” [Online]. Available: https://www.dhakatribune.com/bangladesh/court/2019/03/28/3-659-cybercrime-cases-filled-over-6-years-only-25-punished.

[13] M. M. G. Dr Eva Nagyfejeo, Ms Carolin Weisser, “Cybersecurity Capacity Review,” 2018.

[14] “Digital Security Act 2018.”

[15] K. Sarker, H. Rahman, K. Farzana Rahman, S. Arman, S. Biswas, and T. Bhuiyan, “A Comparative Analysis of the Cyber Security Strategy of Bangladesh,” in International Journal on Cybernetics & Informatics, 2019, vol. 8, no. 2, pp. 01–21, doi: 10.5121/ijci.2019.8201.

[16] S. Kundu, K. A. Islam, T. T. Jui, S. Rail, M. A. Hossain, and I. H. Chowdhury, “Cyber crime trend in Bangladesh, an analysis and ways out to combat the threat,” in International Conference on Advanced Communication Technology, ICACT, 2018, vol. 2018-Febru, pp. 474–480, doi: 10.23919/ICACT.2018.8323800.

[17] A. M. Maruf, M. R. Islam, and B. Ahamed, “Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies,” in Northern University Journal of Law, 2014, vol. 1, no. October 2014, pp. 112–124, doi: 10.3329/nujl.v1i0.18529.

[18] "Natinal Cyber Security Strategy" 2014 [Online] available : https://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf

[19] Mahmuda Akhter Bonnya “Cyber Threat and Security: Bangladesh Perspective,” 2020

[20] "Digital Security , *Handbook on Cyber Security* (pp 55-71)" 2020 [Online] available: http://cbseacademic.nic.in/web_material/Manuals/Cyber_Safety_Manual.pdf

Appendices

Appendix 1: Authors Contribution Assessment

Required Title	Title in current thesis	Pages, Percentage
1.Introduction	1. Introduction	1.5, 3.75%
2. Background	2. Background Study	12, 30%%
2.Methodology	3. Methodology	3, 7.5%
3.Results	4. Result Analysis	23, 57.5%
5.Summary	5. Conclusion	1, 2.5%

Appendix 2: Online Questionnaire

1. Which type of devices are you currently using to access the internet?
   a. Laptop
   b. Desktop
   c. Smartphone
   d. Tablet
2. What type of connection do you use for internet access?
   a. Public Wi-Fi
   b. Personal Wi-Fi
   c. Broadband Internet
   d. Cellular Data
3. How much time do you spend on the internet in a day?
   a. Less than an hour
   b. 1-2 Hours
   c. 2-4 Hours
   d. More than 4 Hours
4. How much are you familiar with computers/internet?
   a. Not so much
   b. Average
   c. Mostly
   d. Professional
5. How many years of IT experience/Education do you have?
   a. Less than a year
   b. 2-5yers
   c. More than 5 years
   d. Did not receive any education
6. What is/are the main software(s) that consumes your most internet usage?
   a. Social media app (Facebook, Twitter, Instagram, etc.)
   b. Online gaming
   c. Online education
7. How do you usually get the essential software?
   a. Buy them officially

b. Buy from local market via CD/DVD

c. Look for free authentic alternative

d. Download from internet

8. Do you use any online Banking system?

a. Yes

b. No

9. Please mention one online service you use most other than banking.

a. Online shopping

b. Gaming

c. Social Engineering

d. Education

e. Other

10. Do you have any idea about Cyber Security Law in Bangladesh?

a. Yes

b. No

11. How did you get familiar with online Security?

a. School/College

b. University

c. Private training

d. Self-taught

12. Please mention any kind of cyberattack you ever heard in the following Sector.

a. Banking

b. Social media

c. Ransomware attacks

d. Other

13. . Please select if you are familiar with any of these attacks

a. Malware

b. Phishing

c. Scamming

d. Man-in-the-middle attack

e. Distributed Denial-of -Service (DDOS)

14. In case of any situation are you able to take the necessary steps to confront any cyber-attack?

a. Yes, I know

b. No, I do not know how to respond

15. What will be your action against any cybercrimes if you encounter in the future?

    a. Contact with the law enforcement agency

    b. Share it with others

    c. Hide it for social respect

    d. Do nothing

16. Do you know how to handle a situation regarding cybercrimes?
    a. Yes
    b. No

17. Do you receive any sex education in school?
    a. Yes
    b. No

18. What is the proper way to have sex education?
    a. Adult websites
    b. School/College
    c. Parents
    d. Other

19. How old are you?
    a. Below 18 years
    b. 18-25 years
    c. 26-40 years
    d. Above 40 years

20. You are a
    a. Male
    b. Female
    c. Other

21. Where do you live
    a. Urban area
    b. Rural area

22. In your opinion, which one is the most urgent Cybersecurity problem in Bangladesh?

23. What do you think the government should do to address it?
    a. Aware people about Cyber Crimes
    b. Introducing Cyber Crime response team
    c. Introducing appropriate law and punishment
    d. Introducing specialize law enforcement team
    e. Other

24. How do you think including IT security education at the Secondary School level will improve the situation in thefuture?

    a. Will be improved greatly

    b. Will be fairly improved

    c. Will not be much change

    d. Will not be much different

25. If you would like to add anything, was not cover please feel free to write

Appendix 3: Offline Questionnaire

1. What is the purpose of your child’s usage of electronic device (Mobile, Computer etc.)?
    a. Educational
    b. Recreational
2. How many hours does your child spend on internet in a day?
    a. Less than an hour
    b. 1-3 hours
    c. 3-6 hours
    d. More than 6 hours
3. Do you check your children’s device history?
    a. Yes
    b. No
    c. Sometimes
4. Do you have any idea about parental control on electronic devices?
    a. Yes
    b. No
5. What is the highest level of school or degree you have completed?
    a. Primary
    b. Junior
    c. Secondary
    d. Higher Secondary
    e. Graduation or above
6. How many children do you have?
    a. 1
    b. 2
    c. 3
    d. 4
    e. More than four

Appendix 4: Experiment Questionnaire

1. Which of the following you think is ok to practice?
    c. Update your software once a year.
    d. Share your personal information in public medium e.g: Facebook, Instagram, twitter
    e. Use multi-factor authentication.
    f. Connect to any public Wi-Fi to save own data
2. Cybercriminals only target large companies. True or False?
    a. True
    b. False
3. When you hit the “delete” key, that means a file is automatically removed from your computer. True or False?
    a. True
    b. False
4. Only people with access to sensitive data need to be trained on the importance of the physical security of files and equipment. True or False?
    a. True
    b. False
5. If you encounter a ransomware attack, the first thing you should do is pay the ransom. True or False?
    a. True
    b. False
6. Which one of these statements is correct?
    a. If you get an email that looks like it’s from someone you know, you can click on any links as long as you have a spam blocker and anti-virus protection.
    b. If you get a message from a friend who needs your school account password, you should never give it out unless the friend says it’s an emergency.
    c. If you get an email from your school asking you to provide personal information right away, you should check it out first to make sure they are who they say are.
7. Suppose you are a student. An email from one of your school employees asks for the name, address, and other information along with your school's credentials. The email says it’s urgent and to please reply right away. You should reply right away. True or False?
    a. True
    b. False

8. Does HTTP and HTTPS make any difference to you?
    a. Yes
    b. No
9. Email authentication can help you against cyber-attacks. True or False?
    a. True
    b. False
10. If you fall for a phishing scam, what should you do to limit the damage?
    a. Delete the phishing email.
    b. Unplug the computer. This will get rid of any malware.
    c. Change any compromised passwords.

Appendix 5: Provided Material [20]

Digital Security

1.What is digital Security?

Tools such as anti-virus software, biometrics, and personal devices, e.g., the secure chip in a credit card or an ePassport are digital security devices because they offer freedom to communicate, work, travel and shop using your digital identity in a way that is secure.

Digital security is an all-encompassing term, which includes the tools to secure technology, assets, and personal identity in the online and mobile world.

2. Security of Devices

Smartphones, laptops, and tablets are all open to wireless security risks. Protect them against cyberattacks

2.1 Common Threats to Devices

Viruses on digital devices are malicious programmed codes that can corrupt the system and destroy the data within the computer. Some of them are described below

Malware: Malware is a type of malicious software designed to gain unauthorized access or to cause damage to a computer without the knowledge of the owner, stealing and even deleting sensitive data, altering, or hijacking computer functions to monitor users' computer activity.

Ransomware: Ransomware is a type of malicious software designed to extort money from the user. The attacker locks the victim's computer system files or blocks access to files or the computer system typically through encryption until the ransom is paid. Paying the ransom is no guarantee that the files will be recovered, or the system will be restored**.**

Your One-Up about Hackers: A hacker is someone who will gain entry into a computer without permission, with the intention to use or exploit technology to cause harm, steal or destroy the data contained in it.

Usually, hackers are well versed with computer technologies by using various applications or programmes that penetrate the defense mechanism employed by the target computer and send back the sensitive information like usernames, passwords, IP addresses and using them to gain access into the computer itself.

These applications or programmes can be in the form of Trojans, worms, malware, and viruses, which will install in the system and compromise its security. After all, if the hacker can gain administrative rights, they are free to do anything with the data contained in the compromised computer system**.**

Several public locations like shopping malls and airports among others offer their customers free access to public Wi-Fi. But public Wi-Fi networks also enable cyber criminals to spy on unwary customers, take advantage of this convenience and intercept their data. They can access sensitive information of users' banking credentials, account passwords and other valuable information.

2.2 Preventing and Countering Threats and Risks

Install anti-virus software and ensure that is updated as regularly as possible. Some computers have built-in anti-virus software too. Always follow the below instructions.

a) **Regularly update software and operating systems**

Web browsers, plugins (Java and Adobe Products) and even Office Suites. It is the most common way hackers and malware try to gain access to devices and your information

b) **Use privacy settings on mobile phones, apps, and browsers**

Privacy settings on social media platforms enable you to select who can access your posts online. Try to restrict access of your profile to your friends only. Remember what you post online remains there almost forever.

c) Verify if the Wi-Fi link is legitimate and safe

Treat all Wi-Fi links with suspicion. Public Wi-Fi is inherently insecure — so be cautious. The Wi-Fi link could also be a bogus link set up by a cybercriminal trying to capture valuable, personal information from unsuspecting users. Don't connect to an unknown or unrecognized wireless access point. Try to use known Wi-Fi links, which are password protected**.**

d) Learn to create VPN to avoid downloading of data through public Wi-Fi

Use your mobile phone to create VPN If you need to access any websites that store or require the input of any sensitive information consider accessing them via your mobile phone network, instead of the public Wi-Fi connection.

e) **Verify if the website is legitimate/authentic**

Avoid logging into websites where there is a chance that your identity, passwords, or personal information may be compromised — for example, online banking services or any websites that store your credit card information. Always keep an eye on the URL and check if the website is marked with HTTPS before you provide any information. If it is not HTTPS do not provide any information if asks.

f) **Download apps from trusted sources like Google play, AppStore**

g) **Keep webcams private**

These devices can sometimes be hacked and used to take pictures or videos of you without your consent. Put a sticker over your webcam, laptop camera, or phone camera when they are not in use

h) **USB Storage Device Use**

- Always eject the device clearly to clear the content from your computer and to avoid damaging your data.
- Always scan the USB device with latest antivirus before accessing.
- Protect your USB device with a password.
- Encrypt the files/folders stored on the device.
- Use USB security products to access or copy data on your USB.
- Do not accept a promotional USB from unknown persons.
- Do not keep sensitive information like username and passwords on the USB

i) **USB Storage Device Use**

Monitor your Bluetooth connectivity. Bluetooth is an amazing feature on many smart devices. However, leaving Bluetooth on while in public places can compromise your privacy. Bluetooth connectivity allows various devices to communicate with each other, and a hacker can look for open Bluetooth signals to gain access to your devices. Keep this function on your phone and other devices locked down when you leave your home, school, or similar secured area.

AirDrop feature allows you to send any kind of content like photos, videos, documents from one Apple device to another wirelessly. It does not impose any restrictions or limits on the file size. AirDrop makes use of the Bluetooth technology to detect and pair with other Apple devices which are located within the range of Wi-Fi and Bluetooth. It is highly recommended to turn on AirDrop only during file transfer

3. Operational Security

3.1 Password

Strong, unique but easy to remember, and private passwords are essential for dealing with unauthorized access to online accounts. The passwords, when shared with another person(s), can be misused. They may be stolen by unauthorized users to collect and misuse your personal information.

Learn how to create strong passwords and passphrases. A password must be difficult to guess. But you should be able to remember it. Writing passwords somewhere is not advisable. Memories it. Your password is given to you to maintain your privacy. Go for an extra layer of security by opting for two-factor authentication (2FA), also known as two-step verification or dual factor authentication. This security process requires the user to provide two different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access.

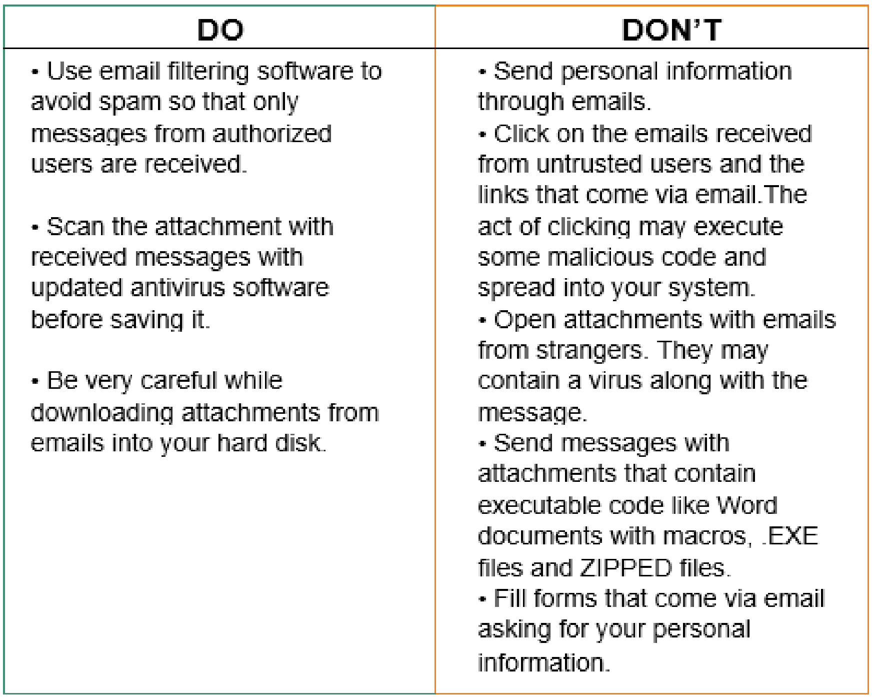
Log out of your account when you plan to be inactive even for a short while. Always keep your system locked whenever it is not in use. You should always remember 3 things about your password-

- Strong
- Unique
- Secret

3.2 Emails and Messages

Most email providers offer filtering services. The use of Rich Text Format instead of the standard .DOC format will retain the formatting but not any macros. This may prevent you from sending virus to others if you are already infected by it**.**

Here is some instruction you should follow.



DO	DON'T
• Use email filtering software to avoid spam so that only messages from authorized users are received. • Scan the attachment with received messages with updated antivirus software before saving it. • Be very careful while downloading attachments from emails into your hard disk.	• Send personal information through emails. • Click on the emails received from untrusted users and the links that come via email.The act of clicking may execute some malicious code and spread into your system. • Open attachments with emails from strangers. They may contain a virus along with the message. • Send messages with attachments that contain executable code like Word documents with macros, .EXE files and ZIPPED files. • Fill forms that come via email asking for your personal information.

3.3 Security Settings on The Browser

- Update anti-virus software regularly
- Adjust the settings in the web-browser. It may limit some functionality but can provide the best protection from malicious content.
- Enable email accounts for multi-factor authentication. Email is the gateway to almost every other account a user may have. When someone loses or forgets an account password, the reset is sent to his or her email.
- Gauge the credibility of the website by checking the URL, lock.
- Look out for warning signals given by web browsers about exposure to a malicious website or content. Such warnings can protect the user from malware, phishing and identity theft. These warnings given by most of the commonly used browsers like Chrome, Internet Explorer, etc. Remember to update your browsers regularly to avoid missing out on such updates.
- Exercise caution while giving details about personal information when registering for access to email accounts, social networks and chat rooms, and free game downloads.

3.4 Data Accessibility and Privacy

Certain online activities compromise the privacy of children

Filling online forms for surveys, contests, downloading games on commercial or free websites. Some websites prompt the user’s fill-up their form for participating in games, surveys, and contests. The name, email id, age, and gender, and at times the telephone number and postal address, obtained in this manner can be used to access information. Some requests are legitimate: much depends on the nature of the website requesting the information. Providing personal information online can result in a student being targeted for spam (unsolicited email), advertising materials and/or viruses. Privacy issues also apply to students developing personal websites and publishing online. Personal details, including photographs of themselves or other students, may lead to the information being captured and reused by others for illegal purposes.

Using secure browsing option when browsing the web reduces your risk of being a victim of cybercrime. Settings and security models are different for each browser.

3.5 Backups

Taking regular data backups is an important strategy for securing all your important data. A backup is the only way to restore the original data.

Why you must have Data Backup

Data on a hard disk can be lost for a variety of reasons, such as:-

-Hardware failure.

-Operating system failure, e.g., file system crash.

-Files or volumes modified or deleted accidentally by yourself.

-Files or volumes modified or deleted intentionally by intruder.

-Files or volumes modified or deleted by virus or malicious codes.

You can also take a backup of your data to keep it safe. Many companies like Apple, Xiaomi, Samsung have inbuilt backup features in their phones.

3.6 Beware of Strangers and Suspicious Links:

Always be very careful about strangers. If someone claim to be your close one and asks for your personal information do not provide any information. Sometimes you might receive some call of some link and they might as you to provide OTP or other personal information. You should never provide any information to them.

4. **Personal Security**

If you would not accept this offline, why would you accept this behaviour online?

If there are people offline who you would be uncomfortable talking to about your physical /sexual experiences, chances are, you'd be uncomfortable doing this with strangers online too. Cyber Groomers who create fake accounts to befriend people, for the purpose of harming them whether physically, sexually, or emotionally.

What you CAN DO with continued harassment:

a) Coming across cyber groomers, your first instinct should be to block and report them on the platform.

b) Do not stay silent, speak to someone you trust who will be able to help. It can be a parent, a teacher, a friend, anyone who you think can give you the support you need to see it through that you are no longer affected by the cyber attacker online. If they are digitally savvy, they will help you implement security measures to stay safe online!

c) Be cautious when your chat partner gives you many compliments regarding your appearance within a short span of your acquaintance.

d) Do not talk to people who ask you to share your sexually explicit photographs or videos. Never accept a friend request from someone you have never met in person. If you share your sexually explicit photos or videos with someone, the person can share those photos with others or post them on social media. They can also blackmail you.

e) Protect your online reputation: Use the services provided to manage your digital footprints and 'think before you post'. Even if offensive posts and pictures are removed by appealing to the service providers, the possibility of someone taking screenshots or downloading the content cannot be ruled out.

People are not always who they say they are. Learn more about protecting yourself when using social media. You should be very careful in the chat rooms. Never share personal details and limit your identity.

f) Take all precautions about sharing personal information and identity details during chats or in public spaces.

g) If groomer is using social media platforms to groom you, you can block him/her. All the social media apps or services have the option to block a user.

h) Save messages, pictures or videos shared with you by the groomer. Such messages, pictures or videos can be used as an evidence to initiate legal action.

i) Your parents/elders can contact local police station to lodge a complaint against the groomer.

j) Do check with your parents before downloading apps or sharing personal information. This is mandatory for anyone below the age of 14. Some apps are malicious in nature. Therefore, to prevent malpractices, it is important to share the information with parents. Also, Facebook policy does not allow any student below the age of 14 to use the app. Even Netflix, YouTube and Amazon Prime mandates 'Kids mode' for all children below the age of 14.

4.1 Abide by The Law

Use reliable services and know how to legally access the music, film and TV you want.

Acknowledge your sources: use trustworthy content and remember to give credit when using others' work/ideas. Think about something you have worked hard for, and imagine that someone online would want to receive the same consideration and receive credit for their work

4.2 Seek Help

Know where to find help: Understand how to report to service providers and use blocking and deleting tools. If something happens that upsets you online, it is never too late to tell someone. Talk to your elders or parents, if your chat partner suggests to keep your conversation with them a secret. You can contact to local police or call 999. Also, you can report an incident here-
https://www.cirt.gov.bd/incident-reporting/

4.3 Dealing with Unauthorized Access

Giving Permissions to apps: While installing apps, give only those permissions that are absolutely essential for the functioning of the apps. Of any application does not function without all permissions, it is best to not install it.

- Sharing the device’s location: Always allow those app with device location permission which actually required.
- Certain characteristics of the digital environment magnify the risk that children will be exploited or abused by other users. In particular, online abusers can easily operate anonymously and bypass gatekeepers such as parents or teachers. When children are bullied online, such as through ‘revenge porn’, their humiliation can be very public.
- Online grooming: deceiving a child for sexual purposes – is on the rise, although its extent remains unknown. The sexual abuse that follows may be online, such as by ‘sexting’ – sending or eliciting explicit sexual images – or offline, if the victim is lured into a meeting.
- Cyber-bullying which takes several forms is becoming more common and can have a profound impact on mental health, well-being, and educational attainment. When children go online, they are more likely to bully others, and to be bullied, than when they are offline.
- Consent Empower children to decide for themselves how others collect and use their information by requiring their consent. As of now, there is no minimum age of digital consent in Bangladesh.

Appendix 6– Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Mohammed Jasim Uddin

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Evaluating Cyber Security Situation in Bangladesh: Inclusion of information security in secondary education”, supervised by Edmund Laugasson
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

07.01.2021

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.