CYBERSECURITY AWARENESS AMONG YOUTHS IN BANGLADESH: A QUANTITATIVE APPROACH

BY

MOSADDEKA AHMAD SRABONY
ID: 232-17-001

This Report Presented in Partial Fulfillment of the Requirements for The Degree of Masters of Science in Management Information System

Supervised By

Dr. Sheak Rashed Haider Noori
Professor & Head
Department of CSE
Daffodil International University

Co-Supervised By

Dr. Md Zahid Hasan
Associate Professor
Department of CSE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

JANUARY 2025

APPROVAL

This Project titled **"Cybersecurity Awareness among Youths in Bangladesh: A Quantitative Approach"**, submitted by **Mosaddeka Ahmad Srabony**, ID No: **232-17-001** to the Department of Management Information System, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of M.Sc. in Management Information Systems and approved as to its style and contents. The presentation has been held on 11th January 2025.

BOARD OF EXAMINERS

Dr. S. M. Aminul Haque — **Chairman**
Professor & Associate Head
Department of CSE
Faculty of Science & Information Technology
Daffodil International University

Dr. Naznin Sultana — **Internal Examiner**
Associate Professor
Department of CSE
Faculty of Science & Information Technology
Daffodil International University

Mr. Md. SadekurRahman — **Internal Examiner**
Assistant Professor
Department of CSE
Faculty of Science & Information Technology
Daffodil International University

Mr. NaziburRahman — **External Examiner**
Technical Lead - Database Administrator,
Wipro Bangladesh Telenor - Grameen Phone

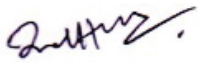
DECLARATION

I hereby declare that this research has been done by me under the supervision of **Dr. Sheak Rashed Haider Noori, Professor & Head, Department of CSE,** Daffodil International University. I also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

Dr. Sheak Rashed Haider Noori
Professor & Head
Department of CSE
Daffodil International University

Co-Supervised by:



Dr. Md Zahid Hasan
Associate Professor
Department of CSE
Daffodil International University

Submitted by:

Mosaddeka Ahmad Srabony

Mosaddeka Ahmad Srabony
ID: 232-17-001
Department of MIS
Daffodil International University

ACKNOWLEDGEMENT

First, I express my heartiest thanks and gratefulness to Almighty Allah for His divine blessing which makes it possible to complete the final year project/internship successfully.

I am really grateful and wish my profound indebtedness to **Dr. Sheak Rashed Haider Noori, Professor & Head**, Department of CSE, Daffodil International University, Dhaka, deep knowledge & keen interest of my supervisor in the field of Machine Learning to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stages have made it possible to complete this project.

I would like to express my heartiest gratitude to **Dr. Md Zahid Hasan**, **Associate Professor,** Department of CSE, for his kind help to finish our project and also to other faculty members and the staff of CSE department of Daffodil International University.

Finally, I must acknowledge with due respect the constant support and patients of my parents.

ABSTRACT

In the modern world, where the use of digital platforms is on the rise, cybersecurity has emerged as a major concern, especially among the young population. Bangladesh being a highly digitized country with a growing number of internet users, so it is important to know the level of cybersecurity consciousness of its youths. This study aims to determine the cybersecurity awareness of Bangladeshi people within the age bracket of 18 to 30 years through a structured survey. To ensure that we get participants of both genders, different levels of education, and those who are residents in urban and rural areas, we randomly selected 250 participants. In our assessment, we wanted to know their perception on the existing cyber threats, their knowledge of the digital safety measures and their frequency of exposing themselves to high risk online. The study shows that there are still gaps in the cybersecurity knowledge and behaviours of the participants, this being affected by the level of socioeconomic status education of the participants. To implement the proper suggestions for the improvement of cybersecurity education and to encourage young people in Bangladesh to adopt safe behaviour in the online environment, the study is presented based on the findings.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1
Introduction

1.1 General Background

In the modern world where people become more and more dependent on the digital environment to communicate, learn, shop, and interact with other people, the role of cybersecurity increases as well. Cybersecurity comprises the measures, techniques, and practices to protect assets, information, and systems from cyber-crises.Youths are most often the main users of the internet, and they are always at risk of falling victim to various cybersecurity threats, including phishing, malware, social engineering and data theft [17] [25].

In Bangladesh, which is going through a process of digitalization, the problem of cybersecurity is relevant and important. As per the Bangladesh Telecommunication Regulatory Commission (BTRC), The number of internet users in Bangladesh has increased dramatically, especially among young people. This group comprises people between the ages of 18-30 years and, comprise a significant portion of the country's online population and are most vulnerable to cyber crimes, hence the need to find out the level of cybersecurity. Although the use of digital platforms has been on the rise among the youth population in Bangladesh, the current level of understanding of cybersecurity among the youth is still scarce. Also, as the use of social media, digital learning, and internet banking increases, the possibility of falling prey to cyber threats also increases for people who are not aware of the preventive measures. It is, therefore, important to understand how young people in Bangladesh perceive digital dangers and interact with online safety to design effective education campaigns. This study focuses on the perception of cybersecurity of the youth, the education system, their online behaviour, and their socio economic background. There are many gaps in knowledge, behaviour, and attitude in this study to contribute to the policy and educational improvement in digital safety [9] [13] [20].

1.2 Problem Statement

This research fills a significant research gap regarding the level of cybersecurity awareness among the youth in Bangladesh. This paper also highlights a major concern that despite the increasing use of the internet, especially through social media and other digital platforms, among the young population in Bangladesh, there is a scarcity of sufficient research which has focuses on the preparedness of the youth to 1face cybersecurity challenges.

This study has a significant implication as it tries to reduce the inequality in the level of cybersecurity knowledge of the youth of Bangladesh. The result will be useful to the policy makers, educators and other stakeholders who are involved in the process of developing programs that will help to increase the digital literacy of this group of people. This study will enable us to come up with proper campaigns and teaching materials that will not only help reduce the risks associated with internet use but also encourage positive internet use.

Also, this research will be of great importance to the existing literature on cybersecurity, especially in the context of developing countries, which is still not well researched. With this work, we expect to enhance the awareness of the youth and make them more self-assured when facing the challenges that come with the use of the Internet.

1.3 Significance of the Study

This study is significant for several reasons:

- **Contribution to Policy Development:** The results will be beneficial in helping government bodies and educational institutions in Bangladesh to make policies and plans that will help enhance the cybersecurity awareness of the youths.
- **Educational Reforms:** The research might encourage the integration of cybersecurity training in academic programs, improving digital literacy in various educational institutions.
- **Enhanced Safety Practices:** Grasping the elements that affect cybersecurity awareness can aid in creating effective strategies to encourage safer online practices among young individuals, thereby decreasing their vulnerability to cyber threats.

- **Academic Contribution:** By concentrating on the context of a developing country, this research will add to the global body of literature regarding cybersecurity awareness and digital literacy in regions that have been insufficiently studied.

1.4 Aim and Objectives of the Study

The primary objectives of the study are:

- To assess the current level of cybersecurity awareness among youths in Bangladesh.
- To identify the key factors influencing cybersecurity awareness, including education, socio-economic status, and digital literacy
- To recommend strategies for improving cybersecurity education and training for youths in Bangladesh.

1.5 Limitations of the Research

A number of problems were there to be faced. Some of them are as follows:

- **The short period of Observation:** The overall period of observation was very short, summing up to a total of three hours only. Hence, a thorough investigation into the study area was not possible.
- **Overgeneralization:** This report is being prepared on the basis of findings from a total of four interviews of the dwellers in the study area. As proper data analysis from all the researchers was not possible to accumulate, the study suffers from a lack of diversity among perspectives.
- **Biased Responses**: The respondents are often found biased toward the issues which we are investigating.
- **Area Coverage by the Researcher:** It was not possible for every researcher to cover the whole of the study area which occupies a large area.
- **Insufficiency of secondary data:** The number of prior research conducted is less. As a second-year student, we had limited knowledge about how to collect data interviewing

respondents. From my point of view, these limitations hampered the project to some extent.

1.6 Conclusion

In order to acquire profound knowledge and practical experience there is no alternative but a field survey. A survey can modify a potential amateur into an efficient person. At the end of this chapter, the aim and objectives of the study have a definite destination.

Chapter 2
Literature Review

2.1 Cybersecurity Awareness

Cybersecurity awareness refers to an individual's knowledge and understanding of potential cyber threats and their ability to take preventive measures to protect themselves and their information online. According to Jones and Colwill [2], awareness of cybersecurity is the first step toward creating a culture of security, especially in younger populations that are more frequently targeted by cybercriminals. Cybersecurity awareness encompasses knowledge of potential threats (for example, phishing, malware, ransomware), understanding of secure practices (e.g., strong passwords, data encryption, two-factor authentication) and recognizing signs of security breaches [5].

Numerous studies underscore the crucial importance of digital literacy in enhancing cybersecurity awareness. This research highlights the necessity for educational institutions to incorporate comprehensive cybersecurity training within their curricula. By doing so, they can cultivate a greater awareness and understanding of cybersecurity issues among students. This strategy equips learners with vital skills to navigate the digital landscape safely and promotes a culture of proactive engagement in protecting both personal and institutional information [11] [10].

In addition, there are now a large number of studies that stress the importance of raising awareness, especially the young, who are at the highest risk of being affected by cyber crimes. The young generation today uses the Internet more frequently than anyone else and is engaged in social media, online games, and shopping, among others, raising many cybersecurity concerns. Youth should be informed of the threats that they encounter in order to be able to effectively address the issue of digital security.

2.2 Youths' Cybersecurity Awareness: A Global Perspective

Researchers worldwide have demonstrated that young people frequently lack sufficient cybersecurity knowledge. In the United States, it has been found that while youths are skilled at navigating digital platforms, they often underestimate the risks4associated with their online activities.

The issue of cybersecurity awareness among youth in the U.S. has gained considerable attention, prompting various studies and initiatives aimed at understanding and improving this crucial area. A recent report indicates that 73% of children and youth aged 8–18 are exposed to cyber risks. It underscores the dual role of young people as both potential victims of cyberattacks and as essential participants in addressing global cybersecurity workforce shortages [27]. Some research has been done to see what cybersecurity problems children and adolescents face in the present world as well as how they can be taught about these problems. The results indicate that awareness-raising systems, particularly self-learning ones, may be useful in the efforts to sensitize the young on cybersecurity [24].

A separate study that focused on the assessment of cybersecurity skills of high school students in Europe revealed that there is a need for more specific educational programs that are in line with the needs of the specific region. In addition, the study revealed that national culture influences the design and impact of cybersecurity awareness programs in various ways, thus calling for more culturally specific approaches. The analysis of cybersecurity awareness in the EU showed that in order to make national strategies more effective, they need to be more specific and in line with the problems of the particular country. Altogether, these research works point to the fact that there is a need for a tailored approach in order to deal with the various issues regarding cybersecurity awareness among the youth in Europe [18] [26].

2.3 Cybersecurity Awareness in Developing Countries

In developing countries there are certain issues that hinder the development of cybersecurity awareness and these include; low digital literacy, unequal distribution of technology, and economic disparities. Many low income youths in countries such as India have poor access to Cybersecurity education hence are at high risks of falling prey to cyber Many criminals. young

internet users in such places are not aware of the dangers that come with using the digital platforms because they have not been trained in cybersecurity.

A review of literature shows that enhancing awareness on cybersecurity is important. One study reviews the role of government, the cooperation between the public and private sector and new technologies in India for the enhancement of education system and cybersecurity training. Some of the studies highlight the fact that social media can be used in teaching children on the dangers and safety precautions of the internet, thus underlining the importance of using simple platforms to raise awareness.

Also, the research indicates that it is crucial to aim the educational efforts at the youth in order to fight the increasing level of cybercrimes. Therefore, the above findings present the need for proper educational programs to enhance cybersecurity awareness particularly to the low income youth in the developing nations [15] [21] [14].

Similarly to many other third world countries, Bangladesh has its share of problems. Many youths in Bangladesh do not have formal training in cybersecurity thus making them easy preys to various online vices. This has been largely attributed to awareness and absence of experts within the country. It has been observed that the growth of cybersecurity professionals has not been on equal par with the increase in internet penetration thus increasing the chances of being hacked [23].

This is a major challenge as the lack of cybersecurity awareness is a big issue. For example, one study explains how government policies, cooperation between public and private sector and emerging technologies in India can contribute to reducing the digital divide and provide equal access to education including cybersecurity training [16]. Also, other researches have focused on the role of social media in the social inclusion of children in teaching them about the digital risks and online safety through the effective use of available platforms. Also, researches of cybercrime show that educational measures targeting young people are efficient in preventing the increasing quantity of cyber threats that they face.

Thus, it is clear that there is a critical need for specific educational initiatives that will raise awareness on cybersecurity specifically among the youth from low income families in the developing countries [19].

2.4 Factors Influencing Cybersecurity Awareness

There are many factors that can affect the level of cybersecurity awareness among the youths [5] [22]

- **Education**: Cybersecurity awareness has a strong relationship with educational achievement. Formal education provides digital literacy and awareness on cybersecurity through various initiatives that are available to individuals who have acquired more educational achievement.
- **Socio-Economic Status**: The youth from wealthy socio-economic background have a better chance of having access to better technology and training in cybersecurity compared to their counterparts from poor backgrounds. Conversely, people from low income backgrounds often do not have access to such resources which increases their chances of being hacked.
- **Digital Literacy**: Another important factor that determines the level of awareness is digital literacy that is the ability to use digital tools. The youths with high level of digital literacy are able to identify the threats and practice safe online habits.
- **Online Behavior**: The behaviors of the young people when using the online platforms determine the risk that they are likely to encounter cyber threats. For instance, those who often use social media platforms, online games, or e-commerce sites may have higher chances of being exposed to cyber threats.

2.5 Common Cybersecurity Threats

It is important to note that young people who are active on the digital platforms and social media platforms are at high risks of being affected by various cybersecurity threats. Such risks usually exploit the interconnectedness and generative nature of young Internet users who may not always be very cautious about security, for instance, to avoid delays or miss out on social interactions. Some of the most dangerous and widespread threats include phishing, malware, social engineering, identity theft, and ransomware. All of these threats are quite dangerous as they can

lead to different outcomes, starting from the personal data theft and ending with the financial loss and the long-term damage to the reputation [12].

2.5.1 Phishing

Phishing has remained one of the most effective forms of cyber attacks in recent years with individuals being the primary target where they are lured into providing sensitive information such as passwords, credit card numbers or even personal identification details through fraudulent emails, messages or websites. The youths are most at risk of falling for phishing attacks because they are always connected and engaged with social media platforms, instant messaging apps and emails which are the primary vectors for phishing campaigns. The youth are generally careless when it comes to the information that they post on the social networks and as such, they become a perfect target for the phishing schemes [8].

Phishing attacks can also come in many forms, including the following:

- **Email Phishing**: The phishing emails are sent from what appears to be a trusted organization including banks or even social media platforms, and they may ask the user to click on a link to verify their account, change their password or enter a competition. The links provided tend to take the users to what seems like a legitimate website where users input their credentials and the information is gathered by the attackers.
- **Spear Phishing**: This is a more specific kind of phishing where the attackers gather information about particular people and then create messages that look authentic. This type of attack is especially effective on young people especially students or professionals since the attackers can use information gathered from their social media platforms to create believable messages.
- **Smishing and Vishing**: Smishing is a type of phishing which uses text messages in order to trick the users while vishing is through voice calls. Both are becoming popular due to the fact that more young people are using their mobile devices to receive information. Some of the smishing messages may include links which when clicked will take the user to either malware infected sites or phishing pages while vishing calls are common where the perpetrators pose as legitimate companies.

Even with the existing awareness campaigns in place, phishing continues to pose a threat, especially to young users who may not be as cautious as they should be [6].

2.5.2 Malware

Malware, which is short for malicious software, is a major threat to the young Internet users. It refers to a broad category of unfriendly applications that have the potential of sneaking, destroying or even seizing control of computer systems. This category comprises viruses, worms, Trojans, spyware, ransomware, and adware. Malware can be transmitted through several modes for example, email attachments, contaminated websites, fake software downloads, and even USB drives. The risky behavior of young people when using the internet including downloading of pirated materials, clicking on unknown links, and using unknown applications makes them fall prey to malware [4].

Youth engagement in risky online behaviors—such as downloading pirated media, clicking on unknown links, or using unverified apps—often leads to accidental malware infections. For instance:

- **Trojans** are frequently masked as authentic software or applications, which may attract younger users looking for free editions of well-known programs or games. After being installed, these applications can obtain sensitive information or establish pathways for attackers to infiltrate the device.
- **Ransomware** attacks have become especially worrying, as malware encrypts a victim's files and requests payment in exchange for the decryption key. Young people, particularly students, may become targets of these attacks if they unintentionally download infected files or access compromised websites. The impact can be severe, resulting in the loss of academic assignments or personal files.

Younger individuals are more inclined than older generations to partake in activities that expose them to malware attacks. This trend is especially noticeable with the rising use of third-party app stores, torrent sites, and streaming services, which tend to be unregulated and may contain harmful content [28].

2.5.3 Social Engineering

Social engineering is any type of influence used to convince an individual to release information or perform an action that may potentially harm them. This is especially dangerous in that it exploits people rather than technical flaws. Young people especially are easily influenced and are very willing to engage with others on the internet, which makes them a prime target for such threats.

Some common social engineering tactics include:

Pretexting: This involves attackers create fake stories or reasons to trick victims into giving up sensitive information. For example, an attacker might pretend to be a friend or a worker from a legitimate company to gain the victim's trust. Young people who often meet strangers online are especially at risk.

Baiting: This involves enticing individuals with appealing offers, such as free music movies, or access to restricted services, in order to lure them into down- loading malware or visiting harmful websites. Young people, who are often attracted to free content, are particularly vulnerable to these traps.

Social engineering is a potent form of manipulation that leverages deep-seated emotions such as curiosity, fear, and urgency to influence individuals. This tactic is especially effective among younger internet users, particularly teenagers and those in their early twenties, who often exhibit a heightened vulnerability to such schemes. Their lower level of skepticism regarding online interactions makes them prime targets for those who seek to exploit these psychological triggers, often resulting in a higher likelihood of falling victim to manipulation [7].

2.5.4 Identity Theft

Identity theft is another significant threat facing young internet users. It involves the unauthorized acquisition and use of an individual's personal information, often for financial gain. With the proliferation of social media, many youths unknowingly expose personal details—such as birthdates, home addresses, and even financial information—that can be exploited by cybercriminals.

Youths are particularly vulnerable to identity theft for several reasons:

- **Oversharing on Social Media**: Young people tend to share personal information on social media sites without giving much thought to the fact that they are posting the information on the internet for anyone, including strangers, to see. Nevertheless, the majority of social media profiles are open to the public and the information posted on them can be gathered by cyber criminals to create impersonation of people or even fake personalities.[29]
- **Weak Password Management**: Most of the young users do not pay attention to the best practices of creating secure passwords, for instance, they tend to use the same password for various sites, or choose very basic passwords that can be easily predicted. This is because the use of easy passwords and similar passwords for different sites makes it easier for cyber criminals to gain control of personal or financial accounts that are linked to such sites [24].
- **Lack of Financial Vigilance**: Young people are not as likely to check on their credit or bank accounts frequently and hence, identity theft can be realized only after some time. This is because they are likely to be slower than the older population in identifying the fraud and thus become easy prey to the identity thieves [1] [3] **.**

2.5.5 Ransomware

Ransomware is a category of malicious software that encrypts a user's files, making them unreachable until a ransom is fulfilled. This danger has intensified in recent years, with educational institutions and individuals being targeted more frequently. Young people, especially students, are at risk due to their dependence on digital devices for both learning and leisure activities.If a student’s laptop or device becomes infected with ransomware, they may lose valuable academic work, personal files, and important data unless they pay the ransom—a payment that does not guarantee the files’ recovery.

Recent ransomware attacks have targeted schools and universities, which often have weak cybersecurity protections. These attacks can directly affect students through their personal devices or indirectly impact them when schools are targeted. The increasing sophistication of ransomware and the availability of ransomware-as-a-service (RaaS) make this threat particularly

dangerous for youths who are less experienced in recognizing malicious downloads or suspicious links.

2.6 Cybersecurity Awareness among Youths in Bangladesh: Review of Research

There is still very little empirical research on the cybersecurity consciousness of youths in Bangladesh and the field of study is rather nascent. However, some research works have been conducted to provide insights into the current state of knowledge and behavior of the youth, indicating the existence of certain gaps. This is especially so given the fast-paced digitization of the country particularly in the use of the internet and smartphones raising questions on the readiness of young internet users in fending off cyber threats.

A study conducted in 2017 examined the levels of cybersecurity awareness among university students in Dhaka. The survey revealed that although a significant number of students frequently engaged with social media and online services, only about 35% demonstrated a fundamental understanding of common cyber threats, such as phishing and malware. Additionally, the research indicated that a limited number of students practiced safe online behaviors, such as regularly updating their passwords or utilizing two-factor authentication. The authors emphasized the necessity for improved educational programs to enhance awareness of cybersecurity risks among young people.

In a separate study, the online behaviors of Bangladeshi youths were analyzed to assess their vulnerability to cyber threats. The findings indicated that approximately 68% of youths admitted to engaging in risky online activities, such as publicly sharing personal information on social media or downloading software from unverified sources. The researchers concluded that low levels of digital literacy and insufficient understanding of cybersecurity practices, particularly among rural and disadvantaged youths, contributed to their increased susceptibility to cyber-attacks.

In a more recent investigation, this study explored the role of educational institutions in raising cybersecurity awareness. They discovered that while university students in urban areas exhibited

higher levels of awareness—largely due to exposure to digital literacy initiatives and coursework in IT—the situation was markedly different for youths in rural areas. The study revealed a significant urban-rural divide, with rural youths being considerably less informed about safe online practices. The researchers recommended the introduction of cybersecurity curricula in secondary and higher education institutions to bridge this gap.

2.7 Role of Formal Education in Shaping Cybersecurity Awareness

Education systems play a pivotal role in increasing cybersecurity awareness among youths. Research by *Chaudhary and Sinha (2019)* demonstrated that schools and universities that integrate cybersecurity training into their curricula produce students with a heightened understanding of cyber risks and protective measures. In Bangladesh, schools and universities have not fully included cybersecurity education in their programs, although some universities now offer information security courses. A well-organized approach to teaching cybersecurity can lower risks and create safer online spaces for students. This study will look at how educational institutions in Bangladesh are helping young people learn about cybersecurity and suggest ways to improve these efforts.

2.8 Conclusion

The literature indicates that while cybersecurity awareness is a global challenge, it is particularly pronounced in developing countries like Bangladesh, where socio-economic disparities and limited digital literacy exacerbate the issue. Understanding education and online behaviors is vital in shaping cybersecurity awareness, and incorporating cybersecurity education into official curricula is a promising approach to enhance knowledge and behaviors. This research aims to build on these insights by investigating the level of cybersecurity awareness among young people in Bangladesh and identifying methods to enhance it.

Chapter 3

Methodology

3.1 Introduction

The methodology describes the procedures to be followed for carrying out research. It also explains the tools/methods to be used and how they will be used for the collection and analysis of information relevant to the research work. The study has used data from primary and secondary sources. Further information has been collected from different sources like books, websites, reports, and studies conducted by donors, the UN, NGOs, etc.

3.2 Types of Data Collected

3.2.1 Primary Data

Primary data was mainly collected through questionnaires, informal discussions, and consultation meetings with the locals and high-ranking officials. The sources were-

3.2.1.1 Observation*:* Observational research is a form of correlational research where a researcher monitors ongoing behavior. There are several varieties of observational research, each possessing its own advantages and disadvantages. These types are categorized based on the degree to which an experimenter interferes with or governs the environment. Observational research is especially common in the social sciences and marketing. It is a method of social research that entails directly observing phenomena in their natural context.

3.2.1.2 Sample Survey*:* A sample survey is a study that obtains data from a subset of a population, in order to estimate population attributes. I made a questionnaire to survey the youth population of Bangladesh. In total 250 respondents were approached with the questionnaires.

3.2.1.3 Personal Interview*:* also called a face-to-face survey, is a survey method that is utilized when a specific target population is involved. The purpose of conducting a personal interview survey is to explore the responses of the people to gather more and deeper information. Personal interview surveys are used to probe the answers of the respondents and

at the same time, to observe the behavior of the respondents, either individually or as a group. The personal interview method is preferred by researchers for a couple of advantages. But before choosing this method for your own survey, you also have to read about the disadvantages of conducting personal interview surveys.

3.2.1.4 Questionnaire*:* A questionnaire is a research tool that includes a series of questions (or other prompts) aimed at collecting information from participants. These questionnaires are often created for the statistical analysis of the feedback, although this is not always the case. They offer benefits over some other survey methods because they are inexpensive, require less effort from the surveyor compared to verbal or telephone surveys, and typically provide standardized responses that facilitate data compilation. Nonetheless, such standardized answers can be frustrating for respondents. Additionally, questionnaires are significantly limited by the need for participants to be able to read and understand the questions and provide answers. We developed two types of questionnaires: one for households and another for focused group discussions.

3.2.1.5 Focus Group Discussion*:* A Focus Group Discussion (or FGD) is a qualitative research method in the social sciences, with a particular emphasis and application in the developmental program evaluation sphere. FGDs are predetermined semi-structured interviews led by a skilled moderator. The moderator asks broad questions to elicit responses and generate discussion among the participants. The moderator's goal is to generate the maximum amount of discussion and opinions within a given time period. We divided it into some parts and conducted a discussion. The workers at the Secondary Transfer Station of the study area took part in it as they share a close relationship with the topic of interest in this research.

3.2.2 Secondary Data

Secondary data is to be used to understand the background of the study area, maps, images, and other relevant information have been collected from BBS census reports, journal articles, books, newspapers, and from various internet sources that are related to the objectives of our study.

3.3 Working Procedure

This includes the way the data to be collected were selected and obtained, the fieldwork and data collection, and finally the processing of the obtained data. Hence the methodology of the fieldwork could be broken down into three major segments:

3.3.1 Pre-field Work Preparations

This part comprises of-

- Topic Selection
- Literature Review
- Research Design
- Preparing Questionnaire

- **Topic Selection-** Selecting the right topic was a huge task, especially considering the limited amount of time allocated to conduct the research work. I wanted to select a topic which is important in the current time as well as goes well with my master's subject. Finally, after a few discussions with my honorable supervisor, we decided to select the current topic keeping all these things in mind.

- **Literature Review-** To get an overall idea about the topic and what research works have already been done on this, a detailed and through literature review of the past research works in this topic was done. It also helped me to find the existing research gap that I was able utilize to proceed with my research so that it can help generate new knowledge on this topic.

- **Research Design-** This study employs a quantitative research design to assess the cybersecurity awareness levels of Bangladeshi youths. A structured survey questionnaire was chosen as the primary method of data collection, enabling the researcher to gather numerical data that can be analyzed statistically. Quantitative methods are particularly effective in capturing broad trends across a population, allowing for a robust analysis of the factors influencing cybersecurity awareness. The study is cross-sectional, meaning data was collected from participants at a single point in time. This approach provides a snapshot of the current state of cybersecurity awareness among youths in Bangladesh.

- **Preparing Questionnaire:** A questionnaire was developed to obtain quantitative and qualitative data about the cybersecurity awareness among youths in Bangladesh. The questionnaire helped to obtain quantitative data to assess the aspects such as Demographic Information, Cybersecurity Knowledge, Digital Safety Practices, and Online Behaviors.

3.3.2 During Field Work

- **Population and Sampling**- The target population for this study comprises Bangladeshi youths aged 18 to 30. This age group is the most active internet user demographic in Bangladesh and is thus most vulnerable to cyber threats. The sample was drawn from universities, colleges, and professional institutions located in both urban and rural areas to ensure a diverse representation of respondents.

  A stratified random sampling technique was used to ensure that the sample reflected the diverse socio-economic and educational backgrounds of the target population. Stratification was based on factors such as gender, location (urban vs. rural), and educational attainment (high school, undergraduate, postgraduate). A total of 250 respondents participated in the study, representing a mix of students and young professionals.

- **Questionnaire Survey:** A questionnaire survey has been carried out simultaneously with the field survey. In total 250 questionnaires were completed. The questionnaire contained both structured and semi-structured questions and collected data on the Demographic Information,

Cybersecurity Knowledge, Digital Safety Practices, and Online Behaviors of the Bangladeshi youth population of different academic levels.

- **Data Collection**- Data collection was carried out using an **online questionnaire** distributed through social media platforms (Facebook, WhatsApp, Instagram) and email. The questionnaire was designed to capture the following dimensions:

1. **Demographics:** Factors like age, gender, level of education, socio-economic background, and geographic location.
2. **Cybersecurity Knowledge:** Understanding of prevalent cyber threats, including phishing, malware, and identity theft.
3. **Digital Safety Practices:** Implementation of strong passwords, two-factor authentication, and routine software updates.
4. **Online Behaviors:** Frequency of engaging in risky online activities, such as exposing personal information on social media, downloading dubious software, or clicking on suspicious links.

3.3.3 Post-field Work Data Processing and Analysis

Collected data were entered into a frequency table and processed for analysis. Primary and secondary data were analyzed both quantitatively and qualitatively. According to the nature of the data and interpreted. Data tables, graphs, and charts were produced and presented in the study findings section. Data acquired from the field survey were processed by using Microsoft Excel.

3.4 Limitations of the Study

- Time constraints in every task were the major problem to carry out this project task.
- Surveyors are not professional and responses vary from person to person which makes the complete study difficult.
- Data can be affected by the characteristics of both respondent and the interviewer.
- The respondent may not provide accurate or complete information.

3.5 Conclusion

To undertake the mammoth task, different groups of people were interviewed. With their collective contribution and my hard work, a successful field study has been undertaken and I was able to produce primary data and summarize the dataset for further analysis which will give an idea about the current status of cybersecurity awareness among youths in Bangladesh.

Chapter 4

Results and Discussion

4.1 Introduction

The major objective of the thesis was to analyze the existing status of cybersecurity awareness among youths in Bangladesh so that it can contribute to policy recommendations and educational programs to improve digital safety. For the field survey, I collected data on four main themes of the study area. They are-

4.2 Demographic Profile

The demographic characteristics of the 250 respondents provide a representative sample of youths from different educational, socio-economic, and geographical backgrounds in Bangladesh. The sample reflects a balanced gender distribution and a diverse range of educational and socio-economic backgrounds, with a slightly higher proportion of respondents from urban areas compared to rural regions.

4.2.1 Gender Distribution:

Among the 250 respondents I interviewed so far were around 51% male, 49% female, reflecting an almost even gender split.

The table 4.1 Gender ratio among respondents presents the gender breakdown of a group of 250 individuals who were surveyed. The data is divided into two categories: Male and Female respondents. There are 128 male respondents, which accounts for 51% of the total respondents. There are 122 female respondents, making up 49% of the total group.

Table 4.1: Gender ratio among respondents

Gender	Number of respondents	Percentage (%)
Male	128	51%

Female	122	49%
Total	250	100%

In summary, the table illustrates that the gender distribution of the survey participants is nearly balanced, with a slight majority of males over females..

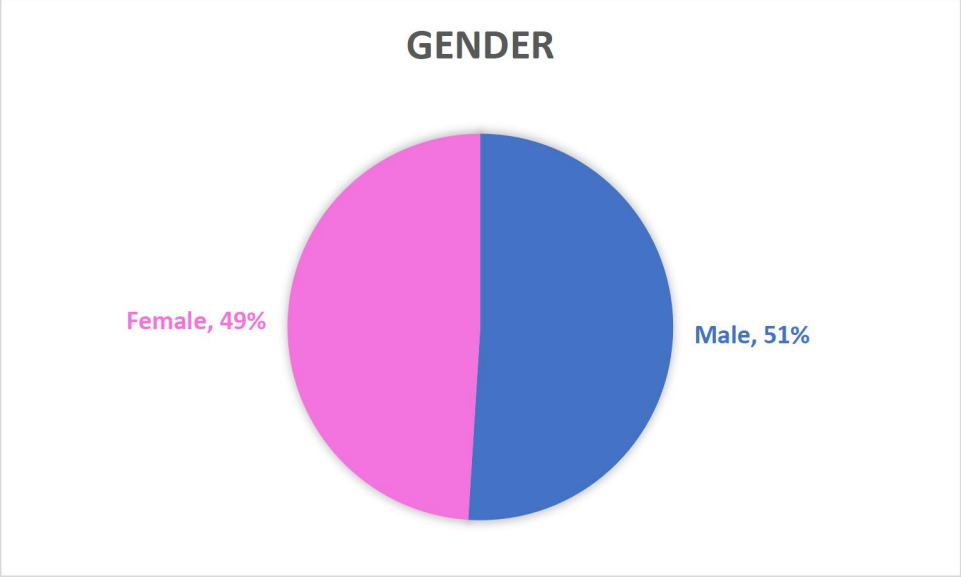


Figure 4.1: Gender ratio

4.2.2 Age Groups:

The majority of respondents fall within the 22–25 years age range, followed by the 18–21 years group, and the 26–30 years group representing the smallest segment. The total number of respondents is 250, and these figures collectively sum to 100% of the survey participants. This distribution highlights the predominance of younger adults (aged 22-25) in the sample population.

Table 4.2: Age Group Distribution of Respondents

Age Group	Number of respondents	Percentage (%)

18–21 years	73	29%
22–25 years	125	50%
26–30 years	52	21%

The following table demonstrates the frequency distribution of age of 250 participants. The data is classified into three age categories: 18–21 years: This age bracket includes 73 respondents, this makes 29 % of the total respondents. 22–25 years: The largest group of 125 respondents, which is 50 % of the total. 26–30 years: This group consists of 52 respondents, which is 21% of the total.

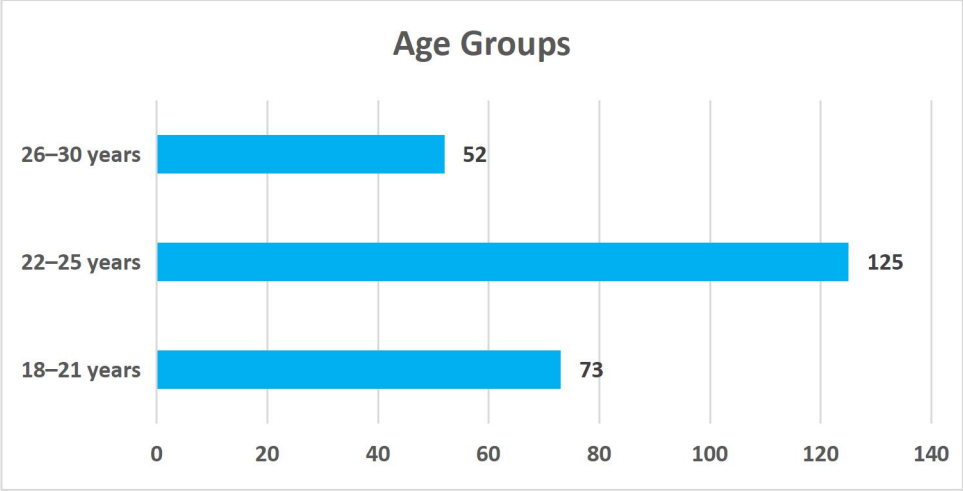


Figure 4.2: Age Group Distribution

4.2.3 Education Level:

Most of the participants are undergraduate students or postgraduate students where the postgraduate students formed the majority of the participants. The high school graduates on the other hand are the group with the least number of participants in this survey. This distribution indicates that the respondents are relatively well educated, more than half of them being undergraduate or postgraduate students.

Table 4.3: Education Level Distribution of Respondents

Education Level	Number of respondents	Percentage (%)
High school graduates	45	18%
Undergraduate students	95	38%
Postgraduate students	110	44%

The following table contains information about the educational level of 250 participants. It shows that the majority of undergraduate the students. participants, The 44%, least are educated postgraduate participants, students, 18%, while are 38% high of school the graduates. participants This are distribution shows that the majority of the participants have sought or are seeking higher education with even greater focus on postgraduate level. The number of participants is 250 and the study involved a diverse group of participants with a high level of academic achievement as the total number of participants.

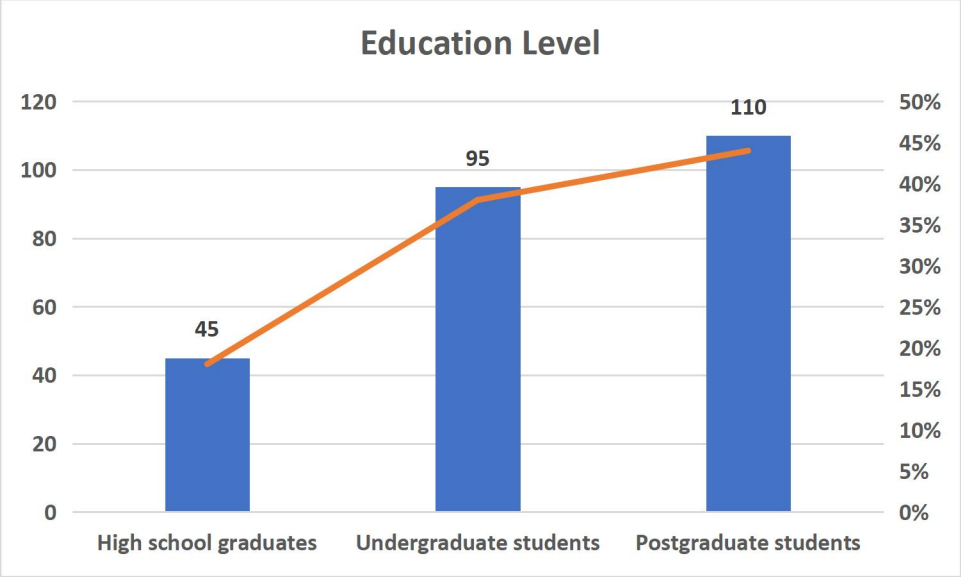


Figure 4.3: Education Level Distribution

4.2.4 Geographical Distribution:

This geographical analysis is therefore useful in providing important information regarding the demography of the sample and reveals a higher concentration of subjects from the urban areas although the rural areas are also well represented. This is where the understanding of the geographical distribution comes in since urban and rural areas have different characteristics and tendencies.

Table 4.4: Geographical Distribution of Respondents

Geographical Distribution	Number of respondents	Percentage (%)
Urban areas	145	58%
Rural areas	105	42%
Total	250	100%

The following table presents the residence locations of 250 participants where there is a visible distinction between living in urban and rural areas. The highest number of participants, 58% (145 people) are from urban areas which means there is higher representation of people from cities or towns. In contrast, 42% (105 respondents) are from rural areas which indicates a relatively smaller figure from the rural or hard to reach areas

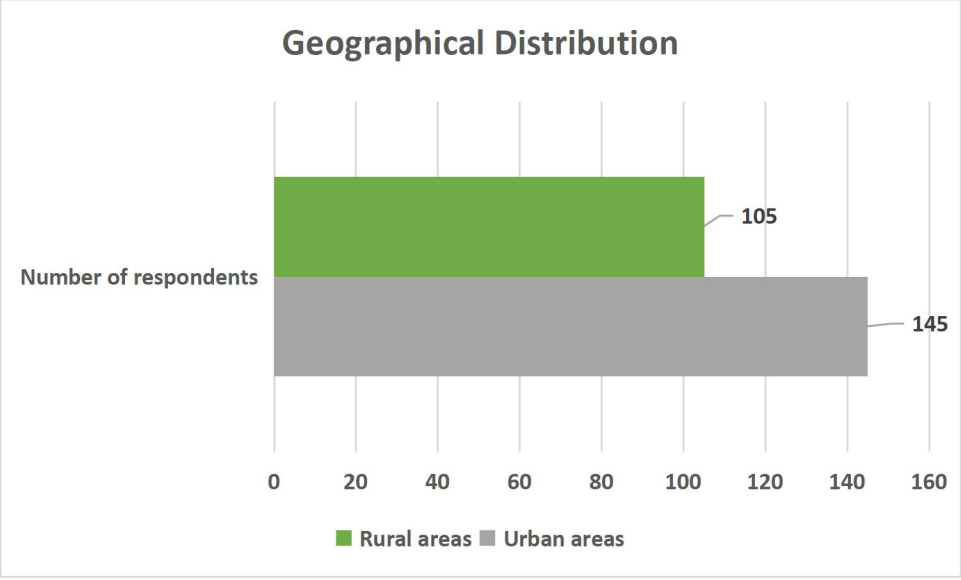


Figure 4.4: Geographical Distribution

4.2.5 Socio-Economic Status:

The majority of respondents belong to middle-income families, followed by a significant number from higher-income families, and a smaller group from lower-income families. This distribution reflects a diverse socio-economic sample, with a clear middle-income dominance.

Table 4.5: Socio-Economic Status of Respondents

Socio-Economic Status	Number of respondents	Percentage (%)
Higher-income family	83	33%
Middle-income family	110	44%
Lower-income family	57	23%

The following table presents the residence locations of 250 participants where there is a visible distinction between living in urban and rural areas. The highest number of participants, 58% (145 people) are from urban areas which means there is higher representation of people from cities or towns. In contrast, 42% (105 respondents) are from rural areas which indicates a relatively smaller figure from the rural or hard to reach areas.

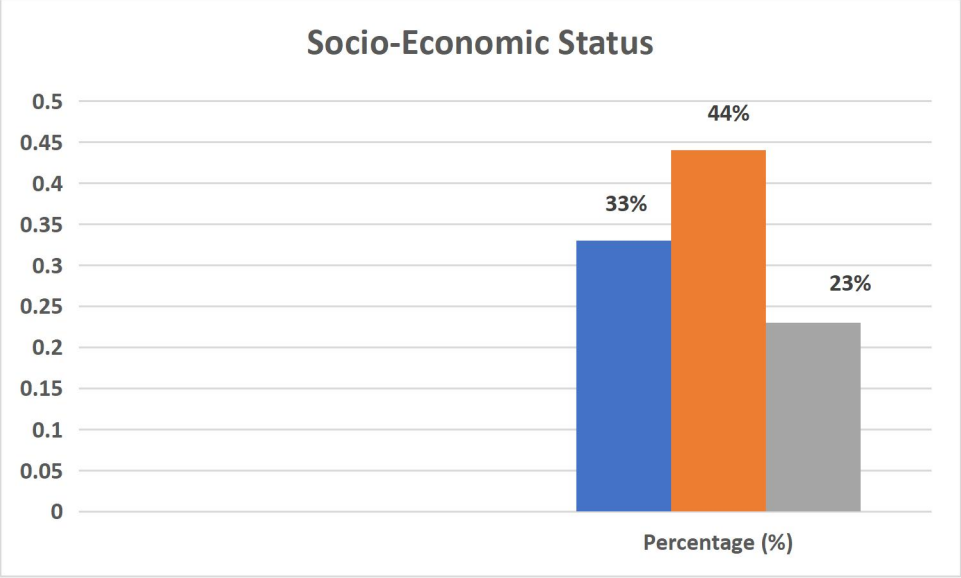


Figure 4.5: Socio-Economic Status

4.3 Cybersecurity Knowledge

The findings suggest that while a majority of respondents are aware of common cyber threats, a significant portion still lacks a deeper understanding of cybersecurity risks and defense strategies:

- **Awareness of Cyber Threats**:
    - 56% of respondents indicated that they were not familiar with common cyber threats such as phishing, malware, and identity theft.
    - However, only 17% could correctly explain how these threats work or how they might protect themselves against them. This indicates a basic awareness but limited technical knowledge of the nature of cyberattacks.
- **Perception of Cybersecurity Risks**:
    - 56% of respondents believed they were at a high risk of becoming victims of cyberattacks, whereas 29% identified as Somewhat vulnerable and 15% as not vulnerable, suggesting a potential underestimation of the dangers posed by insecure online behaviors.

4.3.1 Familiarity with Cyber Threats:

Malware is by far the most widely known cyber threat, while other threats like phishing and social engineering are not very well recognized by more than half of the participants. The results indicate that, although there is a good level of understanding of some threats, there is still a lack of awareness of the more complex varieties of threats.

Table 4.6: Familiarity with Cyber Threats

Familiarity with Cyber Threats	Number of respondents	Percentage (%)
Phishing	15	6%
Malware	130	52%
Social engineering	42	17%
Identity theft	63	25%

The following table contains information about the level of awareness of different types of cyber threats among 250 people. The most well-known threat is malware, where 52 % of the participants (130 people) have heard about it, the next is identity theft which is understood by 25 % of the participants (63 people). Social engineering has been identified by 17 % of the participants (42 people); the least known threat is phishing, only 6 % of the participants (15 people) have heard about it. This distribution shows that the respondents are best aware of the typical threats including the malware and identity theft, however, there is little knowledge about the specific threats like phishing and social engineering.

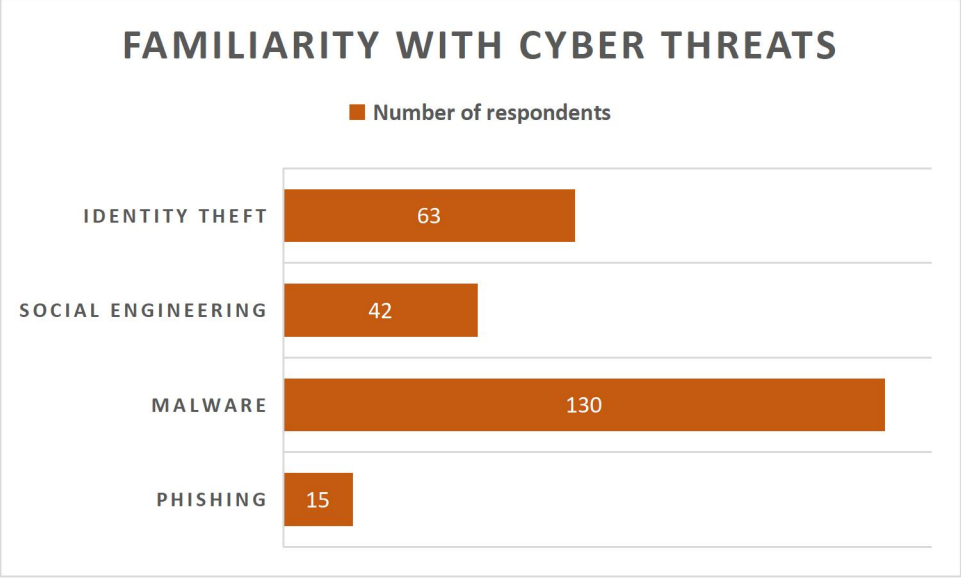


Figure 4.6: Familiarity with Cyber Threats

4.3.2 Explain phishing or malware attacks:

While some respondents are well-informed about these cyber risks, the majority lack a clear understanding, which could point to a need for greater education on cybersecurity threats.

Table 4.7: Explain Phishing or Malware Attacks

Explain phishing or malware attacks	Number of respondents	Percentage (%)
Yes, I can explain both.	42	17%
I can explain one of them.	68	27%
I am not sure.	140	56%
Totals	250	100%

The following table depicts two major cyber threats: phishing and malware. The results show that 17% of the participants (42 respondents) are able to describe both types of attacks, which means that they have a good understanding of these threats. 27% of the participants (68 people) are aware of one of the two attacks; this means that they are partially knowledgeable about the concept. Nonetheless, 56% (140 people) are unaware and have no idea what phishing or malware is, thus showing a huge knowledge gap. This distribution indicates that a very small portion of the respondents is well informed on cyber threats. At the same time, the majority has insufficient knowledge hence calling for more awareness seminars on cybersecurity threats.

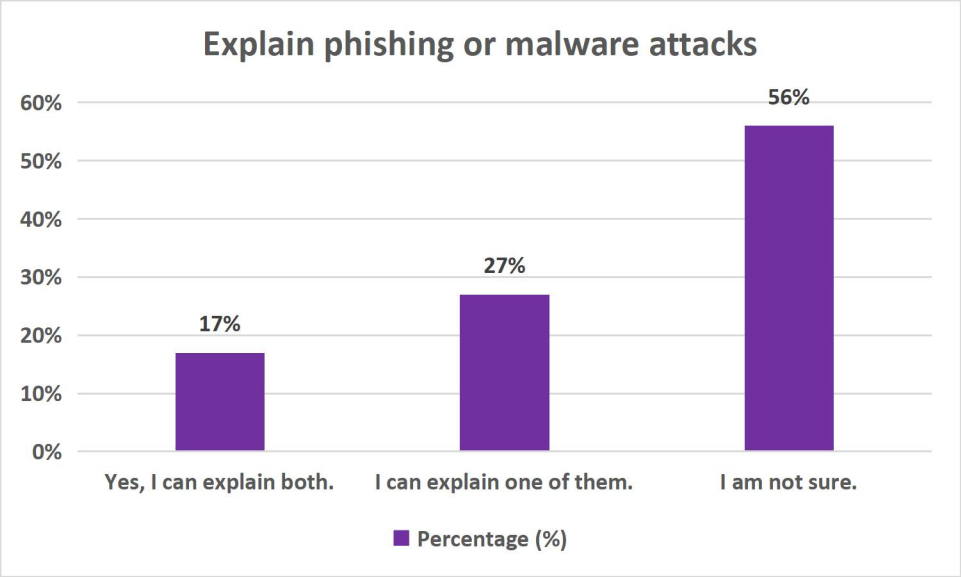


Figure 4.7:Explain Phishing or Malware Attacks

4.3.3 Understanding of Cybersecurity Risks:

A third of the respondents said to have a good understanding of cybersecurity while 61% of the participants have limited or no idea of the risks that are involved. This suggests a major knowledge gap; therefore there is a need to increase people's understanding of cybersecurity and the importance of cyber hygiene to enable people to identify and mitigate cyber risks.

Table 4.8: Understanding of Cybersecurity Risks

Understanding of Cybersecurity Risks	Number of respondents	Percentage (%)
Excellent	15	6%
Good	30	12%
Average	53	21%
Poor	105	42%
No understanding	47	19%

From the table, it is possible to see how participants assessed their knowledge about various cyber security risks. As for the level of their understanding, 42 percent of the respondents scored it as poor,

while 21 percent said it was average. Cyber security is a rather narrow field, and only 6 percent of the respondents stated that they have excellent knowledge in this area; 12 percent believed they were good, 19 percent answered that they had no knowledge in this field, and 12 percent chose the option "I rather don't want to know. " Furthermore, only 6 % of the participants were considered to be experts in the field.

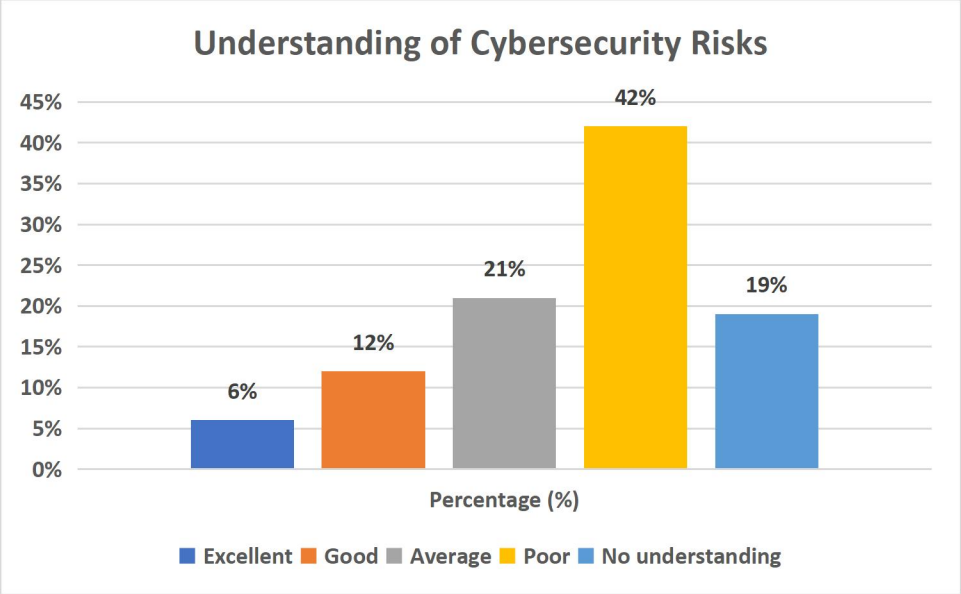


Figure 4.8: Understanding of Cybersecurity Risks

4.3.4 Vulnerability of Cyber-attack:

Of the participants, 50% believe that they are at high risk of being hacked, which shows that the consciousness of the risks of cybersecurity is high. The finding of a lesser proportion of people who reported that they are not vulnerable implies that most people are conscious of or afraid of the risks that they encounter while using the internet.

Table 4.9: Vulnerability to Cyber-attacks

Vulnerability of Cyber-attack	Number of respondents	Percentage (%)
Highly vulnerable	140	56%
Somewhat vulnerable	73	29%
Not vulnerable	37	15%

The table shows that the majority, 56% (140 respondents), perceive themselves as very likely to be hacked, which indicates high level of worries regarding the security of their online data. 29% (73 respondents) said they are somewhat vulnerable, this may suggest an average understanding of the risks that are involved. A third group, 15% (37 respondents), believed that they are not vulnerable at all, this may imply that they do not perceive the threats or are not knowledgeable about cybersecurity. This distribution shows that the participants generally feel vulnerable on the cyber level, although most of them have admitted that they are to some extent at risk in the cyber world.

Figure 4.9: Vulnerability to Cyber-attacks

4.3.5 Encountered Cybersecurity Threat:

Many people have directly experienced cybersecurity issues, a sizable portion remains unaware or unsure of their exposure to such risks.

Table 4.10: Encountered Cybersecurity Threat

Encountered Cybersecurity Threat	Number of respondents	Percentage (%)
Yes	110	44%
No	57	23%
Not sure	83	33%

From the table, it can be seen that 44% (110 respondents) have experienced a cybersecurity threat which indicates that many people have experienced such issues. On the other hand, 23% (57 respondents) said they did not experience any form of cybersecurity threats which means a certain group of people might not have been affected or may not have recognized the existence of such threats. However, 33% (83 respondents) are not sure whether they have been affected by a cybersecurity threat, this may be due to lack of knowledge or ignorance of the matter. In general, the results show that the majority of the participants have experienced cybersecurity threats and some of the others are not sure or have not experienced any threat.

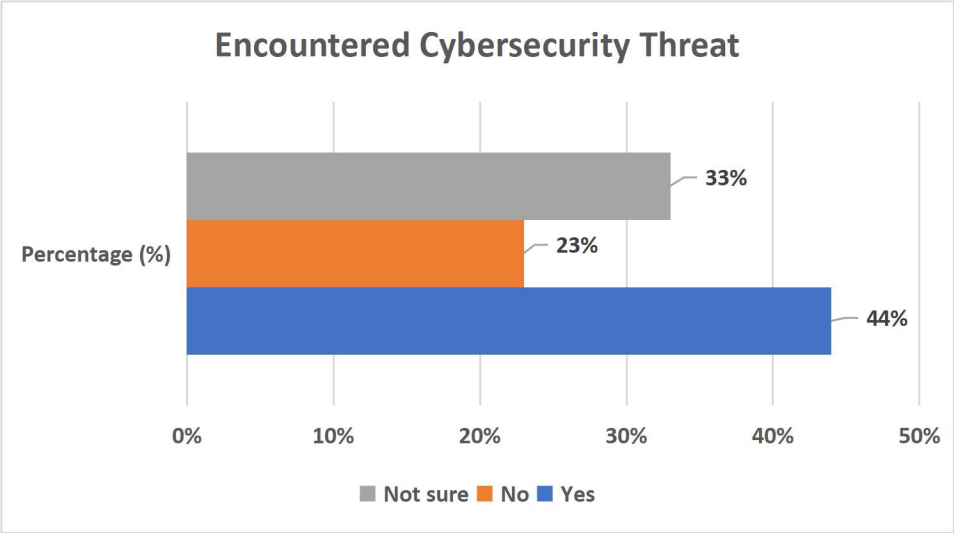


Figure 4.10: Encountered Cybersecurity Threat

This gap between basic awareness and in-depth understanding highlights the need for targeted educational initiatives aimed at increasing youths' knowledge of cybersecurity in Bangladesh.

4.4 Digital Safety Practices

Digital safety practices among the respondents reveal mixed levels of adherence to best practices for online security, with many showing insufficient protective measures:

4.4.1 Password Practices:

Only 19% of respondents reported using strong, unique passwords for their online accounts. However, 44% admitted to reusing passwords across multiple sites, a risky practice that could leave them vulnerable to credential theft or account compromise.

- **Use of strong, unique passwords:**

The high percentage of respondents practicing insecure password habits, there is a clear opportunity to improve online security through better habits and tools, such as password managers and multi-factor authentication (MFA), to mitigate these risks.

Table 4.11: Use of strong, unique passwords

Use of strong, unique passwords	Number of respondents	Percentage (%)
Yes	47	19%
No	93	37%
I use the same password for multiple accounts	110	44%

From the table, it is seen that 19% (47 respondents) always create strong and unique passwords for all their accounts which is recommended for the online security. On the other hand, 37% of the respondents (93 people) do not use strong or unique passwords, which means that their accounts may be at a high risk of being hacked. As for the latter category, 44% of the participants (110 people) stated that they reuse passwords across different websites which is rather dangerous. This data indicates that the majority of respondents do not adhere to the best practices for the password security, thus indicating the importance of enhancing the consciousness level and improving the behaviors to safeguard against the threats of cyber-crime.

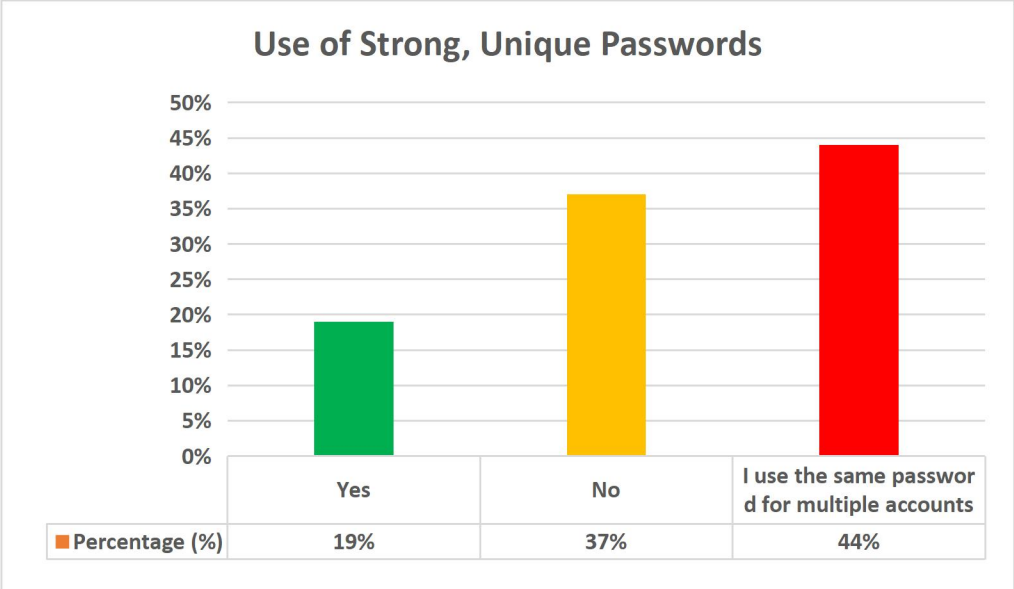


Figure 4.11: Use of strong, unique passwords

- **Frequency of changing passwords:**

Table 4.12: Frequency of changing passwords

Frequency of changing passwords	Number of respondents	Percentage (%)
Every 1-3 months	37	15%
Every 6 months	25	10%
Once a year or less	100	40%
I never change my passwords	88	35%

The data presented in the graph indicates some disturbing password practices by the respondents. As many as 15 % of the respondents update their passwords between the intervals of 1 to 3 months which is considered to be good cybersecurity practices while 10 % update their passwords after every 6 months. Shockingly, 40 % of the respondents change their passwords once a year or even less frequently while 35 % of the respondents never change their passwords which creates a high risk to their accounts. These findings therefore call for improved

sensitization of the public on the need to change their passwords frequently to avoid falling victim to cyber criminals.

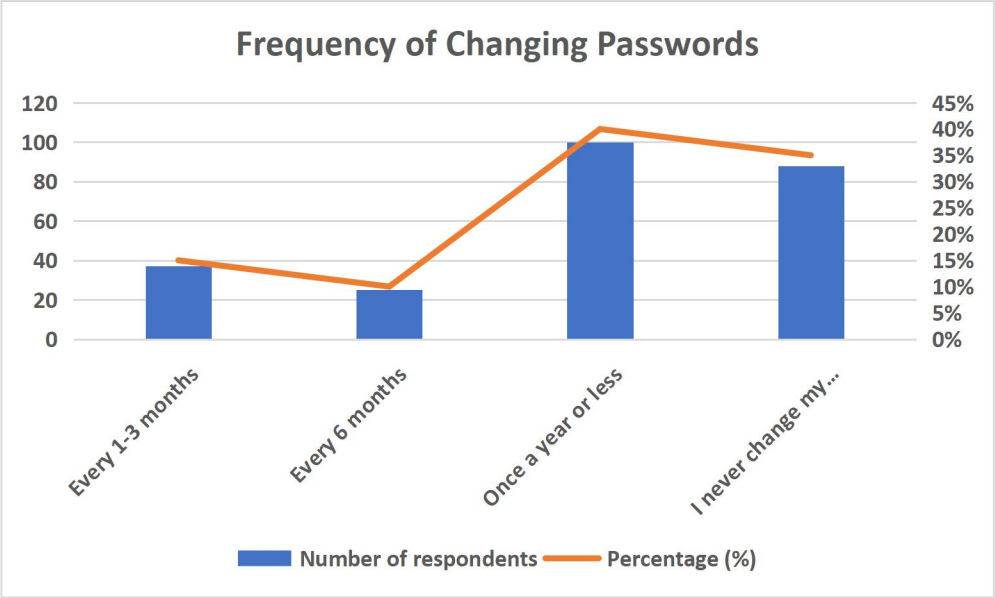


Figure 4.12: Frequency of changing passwords

4.4.2 Two-Factor Authentication (2FA):

Only 23% of respondents reported using 2FA for their important online accounts, such as email or social media. Alarmingly, 37% of respondents were unaware of 2FA, indicating a gap in knowledge regarding this critical security measure.

Table 4.13: Use of Two-Factor Authentication

Use of Two-Factor Authentication (2FA)	Number of respondents	Percentage (%)
Yes	58	23%
No	100	40%
I don't know what 2FA is	92	37%

The data shows that there is a huge difference in the use and knowledge of Two Factor Authentication (2FA) among the respondents. 2FA is a security measure which is not complex at

all and is used to protect accounts by adding an extra layer of security and 23 % of the participants (58 people) stated that they use it. On the other hand, 40 % of the participants (100 people) do not use 2FA and 37 % of the participants (92 people) are not even aware of what 2FA is. This shows that there is still a low level of knowledge and usage to of increase fundamental awareness cybersecurity and measures encourage such people as to 2FA utilize hence it there in is order a to need enhance protection when using the internet.

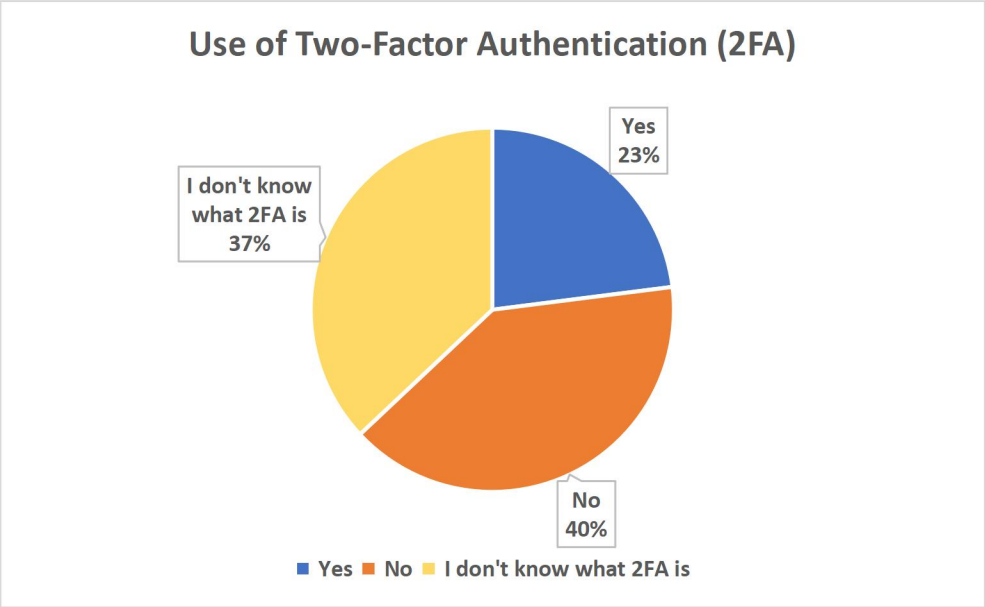


Figure 4.13: Use of Two-Factor Authentication

4.4.3 Software Update Practices:

Only 21% of respondents said they regularly updated their software and antivirus programs. The remaining 53% admitted that they rarely or never performed updates, exposing themselves to potential malware infections due to outdated software.

Table 4.14: Software Update Practices

Software Update Practices	Number of respondents	Percentage (%)
Regularly	52	21%
Sometimes	68	27%
Rarely or never	130	53%
Total	250	100%

The following data represents major concerns with regard to software update practices among the respondents. As you can see, only 21% of the participants or 52 individuals reported to update their software frequently which is advisable in order to keep the system secure and to prevent threats that are associated with vulnerabilities. Out of this, 27% (68 respondents) update their software sometimes while 53% (130 respondents) update their software infrequently or almost never. This suggests a high risk since old software is more likely to be hacked highlighting the importance of updating the software frequently which this study seeks to bring to the attention of the participants.

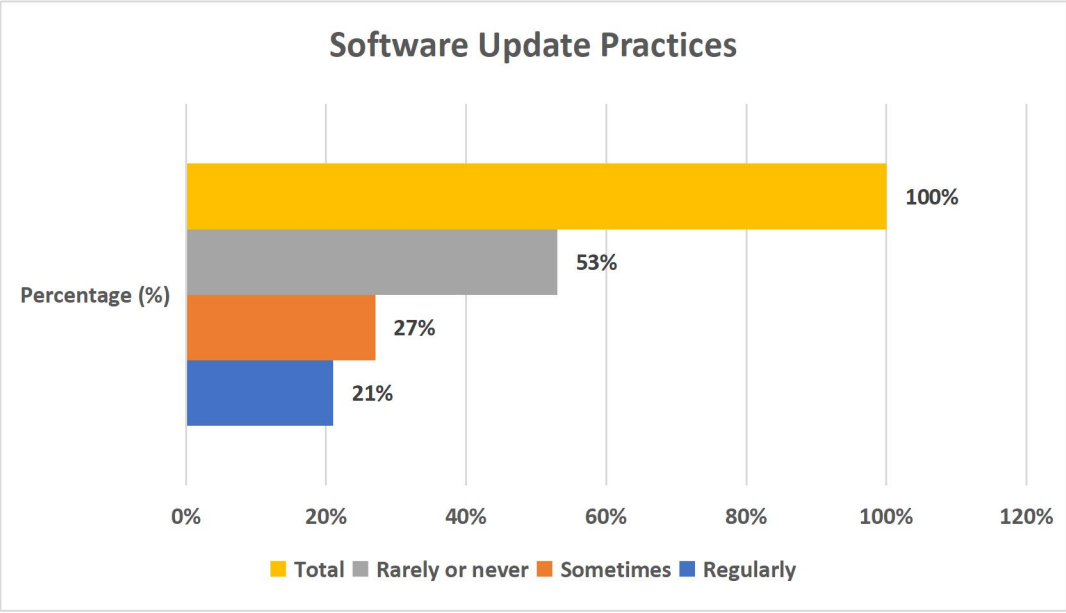


Figure 4.14: Software Update Practices

4.5 Online Behaviors

The online behaviors of the respondents reveal that risky practices remain widespread, even among those who demonstrate a basic awareness of cyber threats:

4.5.1 Risky Behaviors:

42% of respondents admitted to sharing personal information on social media platforms, including details such as their home address, phone number, or date of birth, etc.

- **Sharing personal information on social media:**

Table 4.15: Sharing personal information on social media

Sharing personal information on social media	Number of respondents	Percentage (%)
Frequently	105	42%
Occasionally	67	27%
Rarely	48	19%
Never	30	12%

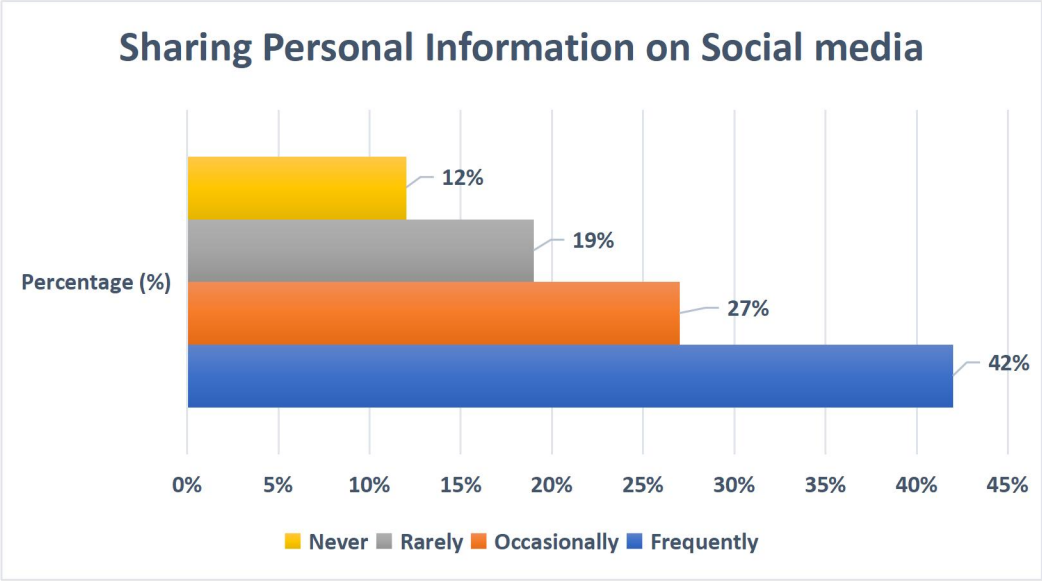


Figure 4.15: Sharing personal information on social media

The data indicate that a large number of the respondents networks. engage Of in the sharing participants, of 42% personal or information 105 when people using share social personal information often; 27% or 67 people share it sometimes. Thus, 19% of the respondents (48 people) do it infrequently and 12% of the respondents (30 people) never do so. This kind of activity increases the probability of identity fraud and other cyber crimes hence the requirement to make people understand the risks of sharing too much information online.

4.5.2 Trust in Online Platforms:

Additionally, 46% frequently downloaded software, movies, or media files from unverified or pirated sources, which could expose them to malware infections or other cybersecurity risks.

- **Download software, movies, or media files from unverified sources:**

Table 4.16: Download software or files from unverified sources

Download software or files from unverified sources:	**Number of respondents**	**Percentage (%)**
Yes, frequently	115	46%
Sometimes	77	31%
No, I only download from trusted sources	58	23%

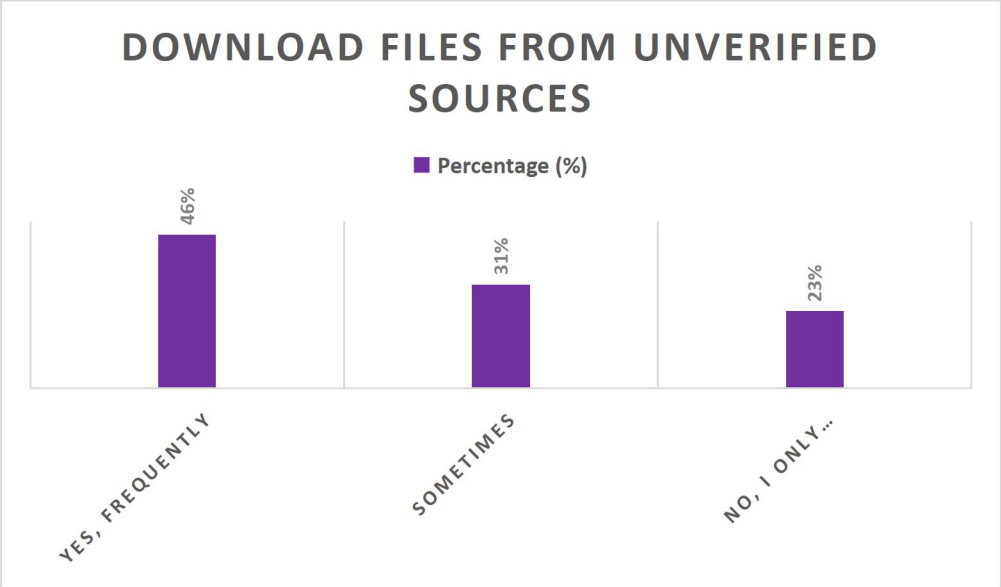


Figure 4.16: Download software or files from unverified sources

The data indicates that there is a risky behavior in downloading software or files from unauthenticated website. As many as 46% of the 252 respondents (115 respondents) often download from such sources while 31% (77 respondents) do so sometimes. This leaves only 23% (58 respondents) who always download from trusted sources. This kind of behavior greatly enhances the chances of contracting malware and other security risks and therefore calls for awareness campaigns to teach people the risks of downloading from unknown sources and the importance of safe browsing practices.

- **Clicking unfamiliar or suspicious links online:**

Table 4.17: Clicking unfamiliar or suspicious links online

Clicking unfamiliar or suspicious links online	Number of respondents	Percentage (%)
Frequently	140	56%
Sometimes	68	27%
Never	42	17%

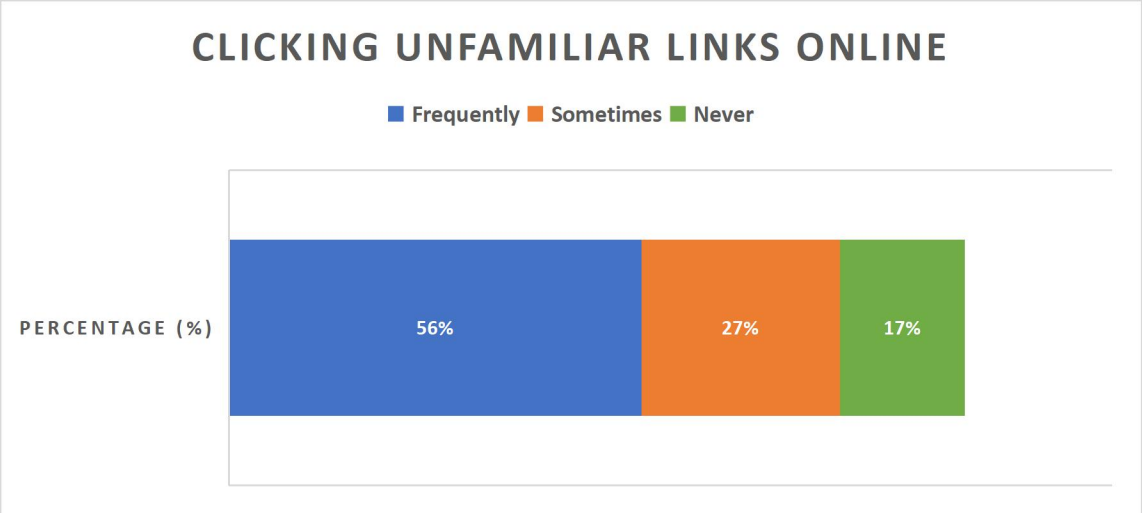


Figure 4.17: Clicking unfamiliar or suspicious links online

The data indicates that many there as is 56% a not of expanded high the or risk participants which of of (140 look clicking the people) dubious on lot, links often and unknown only at click 27% or 17% all. on (68 of potentially This importance links people) the dangerous kind of that click participants links. of awareness they on (42 As behavior campaigns have them people) puts that not do sometimes. users raise not Out in users' click danger awareness on of on such phishing the and risks malware, of therefore clicking highlighting on the unknown links.

4.5.3 Public Wi-Fi Usage:

62% of respondents frequently used public Wi-Fi networks without the protection of a Virtual Private Network (VPN), a practice that could expose them to eavesdropping or man-in-the-middle attacks.

Table 4.18: Public Wi-Fi Usage

Public Wi-Fi Usage	Number of respondents	Percentage (%)
Yes, always	155	62%

Sometimes	63	25%
No, I use a VPN	32	13%

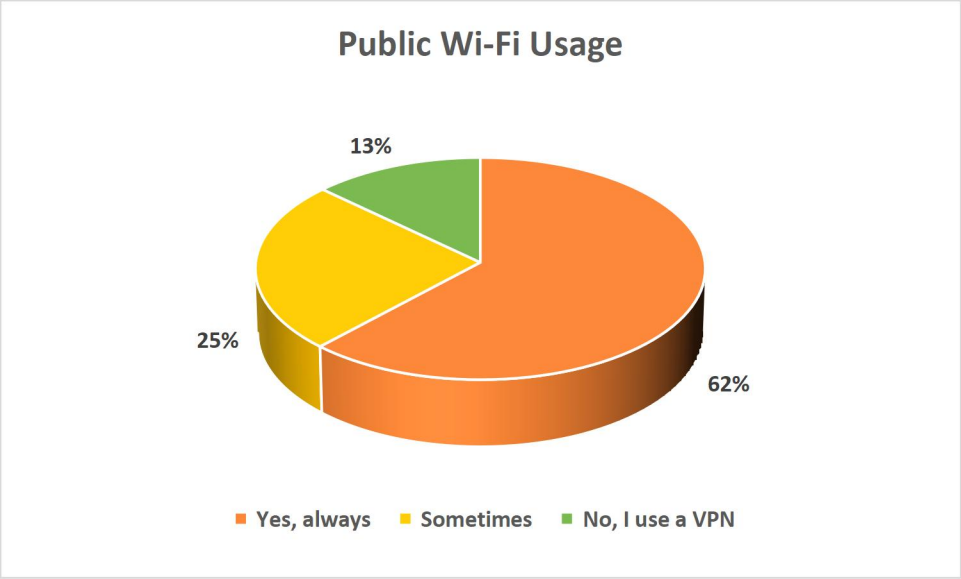


Figure 4.18: Public Wi-Fi Usage

The 62% and data of 25% indicates the (63 high participants respondents) risk (155 do behavior respondents) it when always sometimes. it connect This comes to means to public only public Wi-Fi 13% Wi-Fi without (32 use. adding As other such, security measures respondents) threats, take therefore the there effort is of a using need a to VPN. create This awareness generally on unsafe the behaviour dangers puts of users using at unsecured risk networks of and the importance of using VPNs to secure users' online activities.

The persistence of these risky behaviors, despite a basic understanding of cybersecurity threats, suggests that awareness alone is not enough to mitigate risks. There is a clear need for practical education and training programs that not only inform youths about cyber risks but also encourage them to adopt safer online habits.

4.6 Cybersecurity Education and Awareness

4.6.1 Formal Education or Training on Cybersecurity:

Table 4.19: Formal Education or Training on Cybersecurity

Formal Education or Training on Cybersecurity	Number of respondents	Percentage (%)
Received	92	37%
Not Received	158	63%
Total	250	100%

From the data, it is evident that the majority of the 250 respondents surveyed, i.e., 63% (158 individuals), have not been formally educated or trained in cybersecurity. On the other hand, 37% (92 individuals) claimed to have such education or training. This discrepancy means many people, about 37%, are educated in cybersecurity, but a large number of people, about 63%, are not. This could have consequences for individual and organizational cybersecurity awareness and readiness. The results indicate a possible emphasis on increasing the popularity of cybersecurity training programs to help close this skill gap.

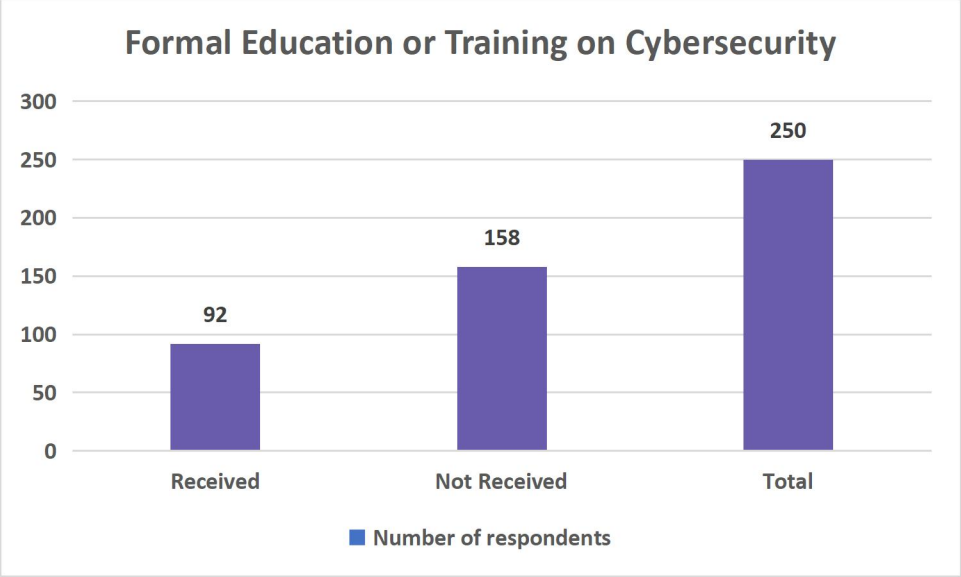


Figure 4.19: Formal Education or Training on Cybersecurity

4.6.2 Interested to Learn more about Cybersecurity Practices:

Table 4.20: Interested to Learn more

Interested to Learn more	Number of respondents	Percentage (%)
Yes	183	73%
No	22	9%
Maybe	45	18%

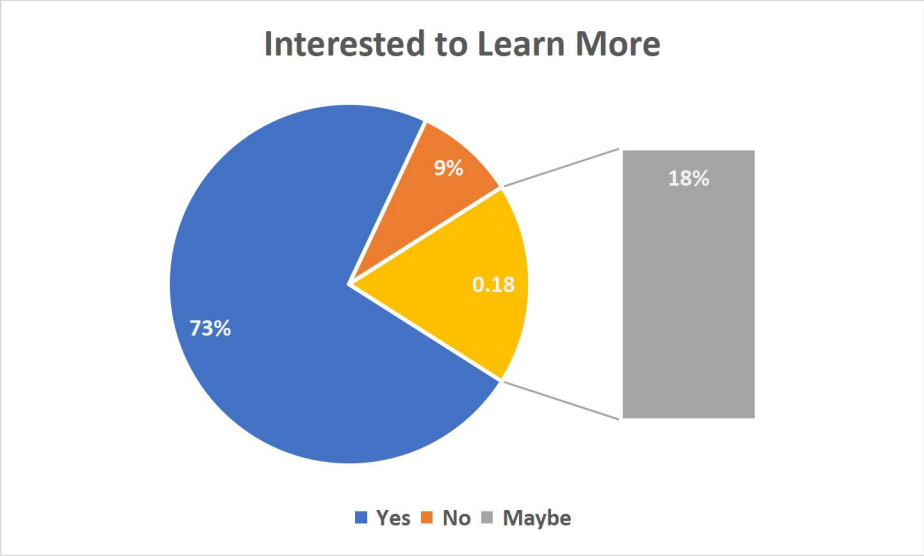


Figure 4.20: Interested to Learn more

The of data cybersecurity. shows When that asked the if participants they have would a like high to level learn of more, interest most, in 73 enhancing % their (183 knowledge in the field people) said that they would, while 18 % (45 people) responded that they were interested but had reservations. This leaves 9 % (22 people) who indicated that they had no interest in the matter. This shows a good potential for the development of educational programs since the majority of people appear to be willing to acquire knowledge regarding how to be safe while using the internet.

4.6.3 Most Effective Way to Improve Cybersecurity Awareness:

Table 4.21: Most Effective Way to Improve Cybersecurity Awareness

Most Effective Way to Improve Cybersecurity Awareness	Number of respondents	Percentage (%)
Educational programs in schools/universities	87	35%
Government campaigns	45	18%
Social media awareness campaigns	68	27%
Workshops and seminars	32	13%
Online tutorials and resources	18	7%

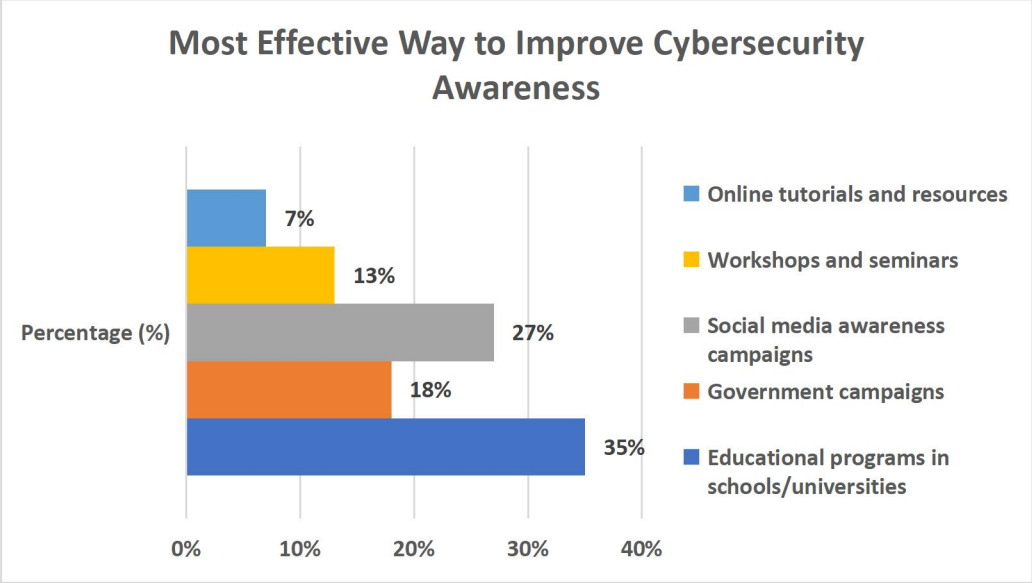


Figure 4.21: Most Effective Way to Improve Cybersecurity Awareness

The data also reveals the best practices for enhancing cybersecurity awareness among the respondents. This is because 35% of the respondents (87 people) believed that this was the most effective measure. Social media awareness campaigns were in the second place with 27% of the vote (68 respondents), government campaigns received 18% of the vote (45 respondents) and 13% (32 respondents) voted for workshops and seminars while 7% (18 respondents) preferred online tutorials and resources. This indicates that the combination of formal education systems and social media platforms would be most effective.

4.7 Conclusion

The results indicate that although a considerable number of Bangladeshi youths recognize cybersecurity threats, a large segment still participates in unsafe online activities and does not possess thorough knowledge of digital safety measures. To close the divide between awareness and implementation, more focused initiatives in education and practical advice are necessary.

Chapter 5

Summary Findings, Recommendation, and Conclusion

5.1 Summary of Findings

This research examined how young people in Bangladesh understand cybersecurity, practice digital safety, and behave online. It revealed key insights into their ability to handle cyber threats. The main findings are:

5.1.1 Cybersecurity Awareness:

Most of they the had participants limited had Thus, understanding fundamental only of knowledge 17% how of of these the the threats cyber participants operate threats could and such explain what these as mechanisms threats phishing are in and in detail. malware, place however, to prevent them.

5.1.2 Digital Safety Practices:

The subject matter of this paper is that participants displayed risky behaviors for instance, password sharing and using not two factor authentication. When it comes to the strength of passwords only 19 % of the respondents indicated that they had strong and unique passwords while 37 % of the respondents indicated that they were not aware of two factor authentication.

5.1.3 Online Behaviors:

Most of the participants reported to have engaged in some behaviours that may be considered as increasing their risk; these include downloading content from unverified sources (46%) and sharing personal information on social media frequently (42%).

5.1.4 Public Wi-Fi Usage:

Out of the participants, 62% of them connected to the public Wi-Fi without a VPN which exposed them to severe risks of data interception and man-in-the-middle attacks.

5.1.5 Cybersecurity Education:

The availability of formal training in cybersecurity was also found to be scarce as 63% of the participants indicated that they never went through any training in this regard. Nonetheless, 73% of the participants showed high level of interest in acquiring more information regarding safe use of the internet.

5.2 Recommendations

To address the identified gaps and enhance cybersecurity awareness among youths in Bangladesh, the following recommendations are proposed:

- **Integration of Cybersecurity Education**:

Educational establishments ought to incorporate cybersecurity awareness initiatives into their programs at both high school and college levels. These initiatives should emphasize hands-on skills, such as recognizing phishing scams, employing two-factor authentication, and adopting safe online practices.

- **Public Awareness Campaigns**:

Government and private entities ought to work together to initiate nationwide cybersecurity awareness initiatives. These initiatives can utilize social media, television, and community workshops to connect with a broad audience.

- **Accessible Online Resources**:

Creating accessible online materials, like tutorials and guides, enables people to understand cybersecurity at their own speed. Engaging elements, such as videos and quizzes, can improve involvement and memory retention.

- **Encouragement of Safe Practices**:

Organizations should encourage people to use safe digital practices. This includes regularly updating software, creating strong passwords, and being careful when using public Wi-Fi networks. To motivate participation, they can offer incentives like discounts or recognition.

- **Targeted Initiatives for Vulnerable Groups**:

Focused efforts must be directed towards rural and disadvantaged youth, as they are frequently more at risk of cyber threats due to a lack of access to digital literacy resources. Community-based training programs and mobile units can help address this disparity.

- **Collaboration with Industry Experts**:

Collaborating with cybersecurity professionals and organizations can help guarantee that training initiatives remain current and proficient in tackling new threats..

5.3 Conclusion

This research shows that there is a high level of cybersecurity awareness among the Bangladeshi youths, however, there is still a great deal of room for improvement. There is a significant knowledge and behavior gap when it comes to cyber threats which shows that there is a general understanding of the threats but not much is being done about it. The outcomes stress the significance of the tailored approaches, both in the sphere of education and within the framework of awareness campaigns, to raise awareness of the proper internet behavior.

Thus, the stakeholders will be able to create a secure environment for the youth of Bangladesh and make them less likely to be affected by cyber threats thus supporting the overall agenda of the country to empower the digital youth. Therefore, future research should assess the impact of these interventions and investigate the dynamics of cybersecurity threats in the context of increasing technological change.

References

[1] J. Ford, “Credit and default amongst young adults: An agenda of issues,” *Journal of Consumer Policy*, vol. 13, no. 2, pp. 133–154, 1990.

[2] C. Colwill and A. Jones, “The importance of human factors when assessing outsourcing security risks,” 2007. [Online]. Available: https://api.semanticscholar.org/CorpusID:54961709.

[3] A. Lusardi, O. S. Mitchell, and V. Curto, “Financial literacy among the young,” *Journal of consumer affairs*, vol. 44, no. 2, pp. 358–380, 2010.

[4] T. J. Holt, D. Strumsky, O. Smirnova, and M. Kilger, “Examining the social networks of malware writers and hackers,” *International Journal of Cyber Criminology*, vol. 6, no. 1, 2012.

[5] M. Whitman and H. Mattord, “Management of information security, 4th edition,” Jan. 2014.

[6] V. Bhavsar, A. Kadlak, and S. Sharma, “Study on phishing attacks,” *International Journal of Computer Applications*, vol. 182, no. 33, pp. 27–29, 2018.

[7] F. Salahdine and N. Kaabouch, “Social engineering attacks: A survey,” *Future internet*, vol. 11, no. 4, p. 89, 2019.

[8] K. D. Tandale and S. N. Pawar, “Different types of phishing attacks and detection techniques: A review,” in *2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC)*, IEEE, 2020, pp. 295–299.

[9] M. M. Hasan, M. R. Islam, and M. S. Islam, “Cyber security awareness in bangladesh,” *ResearchPublish*,2021.[Online].Available:https://www.researchpublish.com/upload/book/paperpdf-1611555745.pdf.

[10] M. Khader, M. Karam, and H. Fares, “Cybersecurity awareness framework for academia,” *Information*, vol. 12, no. 10, p. 417, 2021.

[11] S. AlDaajeh, H. Saleous, S. Alrabaee, E. Barka, F. Breitinger, and K.-K. Raymond Choo, “The role of national cybersecurity strategies on the improvement of cybersecurity education,”

Computers Security, vol. 119, p. 102 754, 2022, issn: 0167-4048. doi: https:// doi.org/10.1016/j. cose.2022.102754. [Online]. Available: https : / / www . sciencedirect . com / science / article / pii / S0167404822001493.

[12] W. Fuertes, D. Ar´evalo, J. D. Castro, *et al.*, "Impact of social engineering attacks: A literature review," in *Developments and Advances in Defense and Security: Proceedings of MICRADS 2021*, Springer, 2022, pp. 25–35.

[13] D. Sun, "Why bangladesh needs to include cybersecurity in curriculum?" *Daily Sun*, 2022. [Online]. Available: https://www. daily - sun. com/ printversion/ details/615994.

[14] C. for Children, "An investigation into the application of social media," 2023, Accessed: 2025-01-01.[Online].Available:https://www.researchgate.net/publication/369278562 Cybersecurity for children an investigation into the application of social media.

[15] A. R. on Cyber Crime, *Some educational suggestions to overcome*, Accessed: 2025-01-01, 2023. [Online]. Available: https://www.academia.edu/49524092/ A Review on Cyber Crime Some Educational Suggestions to Overcome.

[16] D. F. DAI, *Revised campaign final report - sardi sme cybersecurity awareness campaign*, Accessed: 2025-01-01, 2023. [Online]. Available: https://files. digitalfrontiersdai.com/media/documents/Revised Campaign Final Report SARDI SME Cybersecurity Awareness Campaign.pdf.

[17] D. Dave, G. Sawhney, P. Aggarwal, N. Silswal, and D. Khut, "The new frontier of cybersecurity: Emerging threats and innovations," in *2023 29th International Conference on Telecommunications (ICT)*, IEEE, 2023, pp. 1–6.

[18] EPALE, *Cybersecurity and young people: How are things in the eu?* Accessed: 2025-01-01, 2023. [Online]. Available: https://epale.ec.europa.eu/en/blog/ cybersecurity-and-young-people-how-are-things-eu.

[19] T. F. Express, *Human element in cybersecurity training and awareness in bangladeshi msmes*, Accessed: 2025-01-01, 2023. [Online]. Available: https:// thefinancialexpress.com.bd/views/human-element-in-cybersecurity-trainingand-awareness-in-bangladeshi-msmes.

[20] M. M. Hasan, M. R. Islam, and M. S. Islam, "Cyber security awareness among generation z in bangladesh," *ResearchGate*, 2023. [Online]. Available: https: //www.researchgate.net/publication/378909468 Cyber Security Awareness among Generation Z in Bangladesh.

[21] E. R. in India, *Bridging the digital divide in education*, Accessed: 2025-01-01, 2023. [Online]. Available: https://philarchive.org/archive/SHEEEAL.

[22] N. F. Khan, N. Ikram, and S. Saleem, "Effects of socioeconomic and digital inequalities on cybersecurity in a developing country," *Security Journal*, pp. 1– 31, 2023.

[23] T. News, *Bangladesh at risk of cyber attacks due to lack of awareness and expertise*, Accessed:2025-01-01,2023.[Online].Available:https://www.tbsnews. net/bangladesh/bangladesh-risk-cyber-attacks-lack-awareness-and-expertise- 582470.

[24] S. Parimalam, I. F. Kasmin, Z. M. Zainal Abidin, and H. Vasudavan, "Cybersecurity awareness among teenagers and children using self-learning system," *International Journal of Data Science and Advanced Analytics*, vol. 4, pp. 131–138, Jun. 2023. doi: 10.69511/ijdsaa.v4i0.154.[Online].Available:http://www.ijdsaa.com/index.php/welcome/article/view/154.

[25] S. Sharifi, "A novel approach to the behavioral aspects of cybersecurity," *arXiv preprint*, vol. arXiv:2303.13621, 2023. [Online]. Available: https://arxiv.org/ abs/2303.13621.

[26] Sustainability, "Cybersecurity skills among european high-school students," *Sustainability*, 2023, Accessed: 2025-01-01. [Online]. Available: https://www. mdpi.com/2071-1050/14/8/4763.

[27] U.S. Agency for International Development, “Cybersecurity awareness among youth,” U.S. Agency for International Development, Tech. Rep., 2023, Accessed: 2025-01-01. [Online]. Available:https://www.usaid.gov/sites/default/files/2023-10/Cybersecurity%20Briefer Youth.pdf.

[28] K. V. Kumar, V. N. Raju, V. S. M. Reddy, D. Yaswanth, S. Balasubramani, and A. R. GR, “Analysis of cybersecurity awareness among young generation: A research exploration,” in *2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS)*, IEEE, 2024, pp. 1–5.

[29] R. Shabahang, H. Shim, M. S. Aruguete, and A. Zsila, “Oversharing on social media: Anxiety, attention-seeking, and social media addiction predict the breadth and depth of sharing,” *Psychological reports*, vol. 127, no. 2, pp. 513– 530, 2024.

Cybersecurity Awareness among Youths in Bangladesh: A Quantitative Approach

ORIGINALITY REPORT

19%	17%	4%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	docs.google.com Internet Source	8%
2	explorable.com Internet Source	1%
3	www.coursehero.com Internet Source	1%
4	bhairabgangulycollege.ac.in Internet Source	1%
5	Karwan Mustafa Kareem. "The Intelligence Technology and Big Eye Secrets: Navigating the Complex World of Cybersecurity and Espionage", PsyArXiv, 2024 Publication	1%
6	fastercapital.com Internet Source	<1%
7	dspace.bracu.ac.bd:8080 Internet Source	<1%