Article

Cyber Security Awareness among Generation Z in Bangladesh

Farial Ferdous,
***Mehzabul Hoque Nahid**,
Nazia Farhana, and
Azmery Sultana, American International University - Bangladesh (AIUB)
E-mail: mehzab.nahid@aiub.edu

Submission received: 27 July, 2023 / Revised: 30 October, 2023 / Accepted: 01 November, 2023 / Published: 31 December, 2023

Abstract: *This study explores the level of awareness regarding cyber security and cyber threats among generation Z in Bangladesh. Cyber awareness plays a vital role in preventing cybercrimes, which are extremely prevalent these days. This study investigates the threat awareness practices and current knowledge levels among Bangladesh's generation Z. To achieve goals and make it sustainable, it is crucial to know the gap between the number of students with access to technology and those with cybersecurity awareness. This paper will eventually assist in formulating a strong cyber security framework for Bangladesh. A mixed-method approach has been adopted for this case study research to understand the cyber security awareness among business graduates of generation Z in Bangladesh. A thorough literature review helped determine the components of cybersecurity awareness, and a quantitative survey method was used to determine how familiar the graduates were with different cybersecurity practices. Findings indicate that the majority of people are well aware of the cyber threats, yet, most of them are not putting enough effort into avoiding them. In order to manage cybercrime, the study indicates that a model for educating generation Z regarding cyber security is urgently needed. Furthermore, the study portrays an in-depth picture of what generation Z of Bangladesh knows about cybercrime and security measures practices to avoid cyber threats. With the findings of the study, generation Z can get ideas of where they should concentrate more to be more cyber vigilant. As this generation Z is soon to be an integral part of the industry, the policymakers can also develop with frameworks, based on the study findings to educate their employees regarding cyber issues. This research will help outline the gap that needs to be addressed by generation Z and also by others.*

Keywords: Cyber security, Cyber threat, Cybercrime, Cybersecurity awareness, Generation Z, Bangladesh, South Asia.

1. Introduction

The younger generation (generation Z) appears to be less hesitant in revealing their personal information online, whereas the older generation (Millennials) is more cautious about every

----
***Corresponding Author**

detail they share on the platform. This approach may eventually result in a security threat to the members of generation Z.

This study assesses the growing significance of understanding cyber security issues and dangers and aids in the nation's sustainability objectives. It will be necessary to effectively manage cyber security awareness if any nation is to meet its sustainability goals. (Al Mamun et al., 2021). So, this research paper outlays the level of awareness regarding cyber security among generation Z of Bangladesh. It might be difficult to keep personal information secure in this developing world. For a variety of reasons, almost everyone needs to connect to online servers, which requires them to expose their personal information in some way. An organization's Industrial Control System is a crucial component; thus, cybersecurity knowledge is needed to build the framework. More study is needed in this area to close the knowledge gap between what is expected of students and what they really know about cybersecurity (Wang et al., 2022). Cybersecurity is a generic term that is attributed to internet security, information security, and computer security. Understanding the scope, application, and appropriate usage of the internet is crucial. How well-informed a general user is about cyber security issues is referred to as cyber security awareness. Additionally, it describes how they utilize their networks on a regular basis, the risks they introduce and how much security system they use for guarding their electronic devices. Cybersecurity is an international phenomenon that presents a difficult socio-technical challenge for people, organizations, and governments. Although the internet is frequently looked up as a secure medium for exchanging information, conducting business, and regulating the physical world, cyberwars are still occurring, and it is vital to be better prepared. Organizations are spending more money to deal with this growing number of cybersecurity issues. While the majority of cyberattacks are mild, a few have extremely adverse effects. The aftermath of cyber-attacks may range from almost invisible alteration to the system to total disruption of service delivery. As more physical objects are getting connected to the internet to become part of the Internet of Things (IoT) (Chen et al., 2018), it is paving the way for newer ways to attack. Information security uses a similar method of data protection by lowering the information risk. Here Information risk refers to the possibility of a data breach. Data are discrete values that describe an amount, quality, fact, statistics and other fundamental units of meaning, or just sequences of symbols that can be further interpreted. Data plays an important role in our lives. The communication system, information system, and physical infrastructure are all together becoming one unified entity, with newer technologies on the horizon (Ten et al., 2008). An aspect of an information security program that is sometimes overlooked is security awareness. The weakest link in any business is its regular users, who receive very little security awareness training as organizations grow. Because of this, organized cybercriminals nowadays are working very hard to develop cutting-edge hacking techniques that may be used to capture things of value from gullible people (Aloul, 2012).

1.1 Cyber Threat Awareness

Over the past few years, cybercrimes have considerably increased. As the internet and digital systems are developing quickly, it is getting more and more difficult to comprehend the cyber risks. Politicians, ethical philosophers, lawyers, business owners, and other stakeholders are all affected by these attacks, yet many lack the technical expertise required to react to them appropriately. While engineering graduates have a higher level of cyber security awareness, this is not the case for business graduates. Cybersecurity is more important for the business sectors than for any other sector as they deal with sensitive information and valuable assets. In addition to being crucial for students, cybersecurity has a significant effect on institutions. In respect to security tools, this study focuses on the relationships between general human awareness, knowledge, and conduct. An intentional attack was carried out, and it was determined whether the staff members were aware of cybersecurity issues (Shukla et al., 2022; Iqbal et al., 2021). Knowledge of cybersecurity is crucial for long-term solutions and security. It is important to have the knowledge and understanding of cyber security commonalities for business graduates because understanding how communication technology works is a crucial component of their studies. However, cybercriminals frequently target business graduates in their professional lives. The main reason cybersecurity doesn't get the attention it needs seems to be that people find it difficult to communicate about these issues, which has prevented society from responding to attacks in a timely manner. The challenges are:

- Invisible or slight impact
- Lack of robust socio-technical infrastructure
- Vague aftermath of an attack
- Combating the cyber-attack may also invade privacy (de Bruijn & Janssen, 2017).

Due to its widespread deployment and use on different types of devices, the internet—a term that needs no introduction—has become an integral part of daily life. Much of this internet expansion, or what we often use the term "cyberization," occurred in the last ten years due to smart devices like smartphones and tablets. As a developing nation, Bangladesh is extremely concerned about cyber threats. Bangladesh is getting ready to implement a cybersecurity strategy that aims to improve resilience against the growing threat of cyberattacks to encourage the circumstances for the safe operation of cyberspace. Bangladesh is currently taking several significant actions to inform its citizens about the recent cyberattacks and taking the necessary steps to stop the assaults from happening.

1.2 Characteristics of Generation Z

Generation Z, the most recent cohort, has experienced a distinct upbringing in comparison to preceding generations. Many demographic analysts have commonly referred to the current younger generation as Generation Z. Generation Z is comprised of individuals who were born between the years 1997 and 2012. Individuals born between the years 1981 and 1996, encompassing the age range of 23 to 38 in the year 2019, are classified as members of the Millennial generation (Singh, 2017; Dangmei et al., 2016). Conversely, those born in

1997 and onwards belong to a distinct generational cohort referred to as Generation Z. This emerging generation, also known as Gen Z, is currently garnering increased recognition and focus in comparison to preceding generations. Due to the inquisitive nature characteristic of Generation Z, they exhibit a greater propensity for experimentation, a tendency that may have raised concerns among preceding generations (Khan et al., 2020; Mustafa et al., 2018).

1.3 Problem Statement

There is a scarcity of studies evaluating the cyber security scenario in Bangladesh and a greater dearth prevails when it comes to relating it with Generation Z. Hundreds of thousands of new pieces of malware are created daily, whereas trillions of dollars are lost each year due to numerous cybercrimes. Apart from drastic financial losses, breach of personal details brings stress and harm to numerous individuals every day. Different generations' approach to cybersecurity is different than one another. The significance of knowing cybersecurity has grown as the world expands and becomes more technologically interconnected. In fact, higher education in cybersecurity is expanding along with the importance of cybersecurity knowledge (Hunt, 2016). Sustainable development can be maintained if the gap between students' knowledge levels in cybersecurity can be minimized by putting more emphasis on higher education. While the previous generation (Millennial) are more sincere about their personal information, whereas the younger generation (Generation Z) seems to be fine with sharing their personal information, which can sooner or later lead to a very serious threat for Generation Z. A systematic review of scientific studies published on cybersecurity awareness around the world has been conducted to prepare the survey questionnaire. Very few studies on cyber security awareness issues on youth have been captured by that systematic review study (Rahim et al., 2015). One significant study on cyber security awareness among university graduates in the United States has been conducted, and researchers discovered that sentiments of vulnerability among youth were strong markers of a desire to use online with caution (Whitman et al., 2012). However, there is a dearth of research on this arena and that inhibits simulating proper plans and programs to protect this tech-savvy generation from online predators. Several studies indicate that generation Z awareness levels for cyber threats are not as high as anticipated and are often less attentive towards online security activities. In addition to this, nations such as Saudi Arabia, India, Israel, Slovakia, Malaysia, and others have performed more extensive research on the same topic among the general population (Alotaibi\ et al., 2016). Those studies were primarily focused on Cybercrime awareness, Cybercrime concerns, Government involvement, Cybersecurity awareness, and the future of Cybercrime. According to the analysis of previous data, there is a population gap. Bangladesh's cyber security awareness is mostly inadequate and understudied. The University of Dhaka's generation z graduates exhibit a reasonably secure interaction in terms of avoiding dangerous traits, according to research that was conducted to investigate their information security behavior within smartphone owners (Nowrin & Bawden, 2018). In order to comprehend cyber security consciousness to a larger level, more research is required that includes graduates from generation z at multiple universities. This cyber security knowledge among generation z graduates from reputable business institutions in Bangladesh appears to be significant and worthy of further examination, considering their prospective contribution to the employment sectors of Industry 4.0 (Vladimirovna & Zayed, 2021).

1.4 Research Objectives

The main objective behind conducting this research is to originate a more cautious behavior among the generation z toward cyber security activities. Moreover, there are some more objectives of this research, as listed below-

- To undertake an empirical literature analysis on Generation Z's knowledge of cyber security issues and the relevance of cyber security awareness.
- To investigate the level of awareness on cyber security issues among the business grad uates of generation Z from reputed business schools of Bangladesh.
- To offer a brief empirical study on people's awareness of the danger of being victims of cybercrime and their knowledge of the tactics for mitigating that risk to get around problems with cyber security.
- To understand how the population of this study is motivated to protect themselves from the threat of cybercrimes prior to their professional journey.

1.5 Research Questions

According to the research goal, there is a major research gap in the applicability of cyber security knowledge and the understanding of the Generation z's concerns regarding cyber security in Bangladesh. Because of this, it's crucial to ask questions to evaluate the generation-level z's of awareness. Thus, the purpose of this study is to respond to the following questions. –
RQ1: What is the level of awareness generation z BBA Graduates have about cyber security issues and the consequences of cybercrimes?
RQ2: What is the extent of cybercrime victimization awareness among BBA graduates belonging to the Gen-Z cohort, and to what degree are they equipped with the necessary knowledge and strategies for mitigating the associated risks and challenges pertaining to cybersecurity?
RQ3: What factors motivate Generation Z BBA graduates to safeguard themselves against the peril of cybercrime prior to entering the workforce?

2. Literature Review

Everyone who uses IOT (Internet of Things) devices is now increasingly concerned about the constantly changing nature of cyber threats and the growing societal concern about cyber security issues like social engineering, phishing attempts, identity theft, etc. Following a review of numerous research studies on cybersecurity awareness, it was discovered that there are several excellent studies that offer concepts and information that may be used in this research. A British businessman and startup pioneer named Kevin Ashton developed the idea for the Internet of Things in 1999 to describe a system where physical objects will interact with each other using myriad sorts of sensors. Nearly ten years later, in the years 2008 and 2009, there were more devices linked to the network than individuals around the world. Cisco claims that this is the genuine beginning of the "Internet of Things," also known as the "Internet of Everything." According to this method, a system is made up of everything that may be handled as a variable, including people, processes, data, animals, and even atmospheric phenomena (Witkowski, 2017).

2.1 Technology Nowadays

Technology is essential to our everyday lives. It has evolved into one of the most crucial necessities for everyone's life nowadays. It now plays such a large part in our daily lives that it is difficult to picture existence without it. It essentially has an impact on every aspect of our life, including how people learn, study, work, communicate, think, and reflect. In 1998, Mark Weiser of the Xerox Palo Alto Research Center created the phrase "ubiquitous computing." It creates an environment where people can seamlessly integrate and communicate back and forth between the real world and the electronic world from anywhere and everywhere. The article "Understanding Generation Z Cyber Knowledge and Cyber Threat Awareness among Generation Z in Bangladesh" analyzes the problems and reasons for users' lack of cybersecurity awareness based on their age, internet usage, and operating systems”. The article "How Internet Users' Privacy Concerns Have Evolved Since 2002" details how public knowledge of this issue has grown (Antón et al., 2010). This paper will also define the increased popularity of these security issues among users. Another article named “A survey of IoT cloud platforms” informs about the attacks which can occur on Internet of Thing (IoT) devices and how the user can protect their devices from those malicious attacks on everyday life (Ray, 2016). In this paper, this issue has been covered as well by informing the type of the attack and why these attacks are occurring as well. How the level of willingness to explore the internet is influenced with increased awareness regarding the nook and corner of the internet has been discussed in the articles "Cybersecurity awareness framework for academia" and "The impact of internet knowledge on college graduates' intention to continue using the internet," and it is described how the graduates are aware of the issue of cyberthreats and how they are actually protecting themselves from being attacked. This new issue has been dealt with in a specific way in this instance. Here, a variety of factors are presented to support a conclusion regarding academic institutions' cybersecurity awareness (Khader et al., 2021; Wei & Zhang, 2008; Mamun et al., 2013). Since the majority of generation Z graduates are now enrolled in school and primarily use the internet for academic purposes, this essay will outline the benefits of being secure even for these purposes.

2.1.1 Internet Usage Frequency

The internet has effectively integrated into modern society's way of life. Because the internet is the best tool for international communication, information, and entertainment, the number of user involvement has increased tremendously among educated people (Anderson et al., 2017; Hossain et al., 2015). According to research conducted in Bangladesh (Hassan et al., 2020), the male population seems more engrossed with the internet (31.58%) than their female counterpart (21.74%). It's possible that in comparison to women, men tend to be more passionate about learning about just the unknown or discovering new technologies or because they tend to be more drawn to addictive products like pornography, cybersex, and online gaming. In our modified model, the family economic position was identified as a significant predictor of internet addiction, and it was discovered that internet addiction was negatively correlated with excellent economic health.

2.1.2 Internet Knowledge Level

Internet knowledge is described as a collection of capabilities that emerge over time and can be transferred from one application to another (Wei & Zhang, 2008; Mia et al., 2022). What individuals know about the internet and what they can do with it make up the two components of internet knowledge that are crucial to the most popular usage of the internet (Macdonald & Uncles, 2007). Declarative knowledge and procedural knowledge are other names for these two types of knowledge (Macdonald & Uncles, 2007). Declarative knowledge is being familiar with and having the capability to understand internet jargons, whereas procedural knowledge is the capability to carry out certain internet tasks. The knowledge of cybersecurity is crucial for that because students will be the focus of any organization's sustainable development. However, students' knowledge levels aren't all that satisfactory (Alharbi & Tassaddiq, 2021; Nahar et al., 2020). Internet experience is different from internet knowledge, however. The former refers to one's knowledge, whilst the latter refers to one's actions. Even those with the same amount of online experience may have varying degrees of proficiency. People's understanding of the internet may also be influenced by other factors, like demographics and personalities. The connection between the two is obvious: one will often learn more about the Internet as they have more online experience. However, internet experience is only one of the elements that go into developing Internet expertise (Wei & Zhang, 2008; Chowdhury et al., 2023; Hossain et al., 2016).

2.2 Cyber Security

The process of securing electronic equipment, systems, networks, hostile data attacks, etc., is known as cyber security. Everyone who uses an electronic device—from individuals to commercial organizations to governments—should be concerned about cyber security. Cybersecurity entails lowering the possibility of a harmful assault on networks, software, and computers. Tools for detecting break-ins, preventing infections, blocking unauthorized access, enforcing authentication, enabling encrypted communications, and countless more tasks are included (Diakun-Thibault et al., 2014). The definitions of the widely used phrase "cybersecurity" vary greatly, are frequently arbitrary, and may provide little useful information. Technology and scientific advancements are hampered by the lack of a clear, widely accepted definition that captures cybersecurity's multifaceted nature, which validates the field's predominately technical perspective while dividing disciplines that ought to work together to address cybersecurity's complex challenges (Craigen et al., 2014; Zhaltyrbayeva et al., 2021).

2.3 Cyber Threat Reasons

Depending on user needs, the internet is used for a variety of things, including communication, research, education, financial transactions, threading, and more. The most profitable and secure criminal activity now takes place on the internet. Electronic crimes, sometimes known as cybercrime or e-crimes, are unlawful action computing and communication instruments. (Shehab et al., 2020). The rate of E-crimes has seen a tremendous upward curve, inflicting damage to governmental institutions, business organizations, society, and individuals at large (Broadhurst et al., 2014). While trying to pinpoint the reasons why hackers or cyber criminals attack, researchers have ended with numerous motives, including monetary profit and personal vengeance to the lack of stringent laws and policies for cybercrimes (Alansari et al., 2019; Fedotova et al., 2021).

2.3.1 Technological Factor

Cyber-attacks can occasionally be caused by technological flaws. Regardless of the form and kind of connectivity, the weak protection structure of IoT devices has been a concern for security personnel worldwide. Most users look for IoT devices that will make their lives easier to have easily manageable features. By utilizing software-assisted networking, such scenarios are feasible. However, a significant problem with software-assisted networking is zero-day vulnerabilities. Zero-day vulnerabilities are highly harmful to IoT networks due to the deployment and configuration levels of the networks. A zero-day assault can result from the exploitation of a zero-day vulnerability (Singh, 2017). The term "Zero-day" was created in view of the extremely short amount of time that is available to mitigate these risks. The success of developing an update for a malfunction depends on the amount of time that has elapsed since the malfunction got known to the public. The population who deters from installing newly available updates for their software, fuel this trouble even more. Users of a specific application must promptly update to stable releases once a vulnerability is made public. But failing to do so results in a range of negative effects, including cyberattacks (Lamba et al., 2016).

2.3.1.1 Internet Connector and Device Usage

The telecommunications sector of the network industries provides voice and data transfer services, including internet and telephone (both fixed and mobile). The information technology sector, which includes sectors like software and hardware, multimedia sectors like broadcasting and cable television, and sectors connected to delivery services, are some of the industries included in the network industries. Extraordinary success has been achieved by mobile computers, such as laptops, tablets, and smartphones, in large part because of the prevalence of wireless connectivity. Universal and transparent access to the internet and cloud-based apps is made possible through widely used Wi-Fi and cellular networks. The success of mobile computing has been fueled by this.

2.3.1.2 Internet Usage Purpose

Nowadays, practically every facet of daily life involves the internet, whether it’s for work or leisurely activity. For recent generations, digital literacy has become an absolute necessity for both work and regular interactions (Anderson et al., 2017). Social websites were found to be the most popular among internet users in Bangladesh, and many of them (35.2%) preferred to spend more than 3 hours every day online (Hassan et al., 2020). Numerous internet applications showed substantial long-term predictive relationships with PIU. Specifically, among teenagers and emerging adults, playing online games on the Internet was a consistently reliable predictor of PIU.

2.3.1.3 Common Operating System

The number of smart gadgets is currently expanding quickly around the globe. They integrate with consumers' daily lives and offer a lot more amenities to them. For the last ten years, mobiles have been using the centralized cell phone network for personal communication. Smart phones are created technically to be very practical for end users. Strong cellular networks enable us to communicate with each other with text, photographs, voice messages, and videos today. The internet can be easily accessed by a smart phone to send and receive data over the cellular network. The intelligent items are gadgets with built-in software, sensors, and programming. By means of internal programs, each smart object has a unique identifier in the network (Alam, 2018). Billions of devices around the world make use of a few very common operations systems, which becomes a sitting duck target for hackers for invasion.

2.3.2 Human Factor

The development of technological defenses against cyberattacks takes a lot of time and work. However, organizations continue to experience alarmingly frequent disruptions due to serious flaws and significant system breaches. Human mistakes are mostly to blame for the disorder. Since successful phishing attacks rely on tricking a user into believing unreliable sources, they fall under the category of human error. In the 2016 report, phishing and malware were ranked first and second, respectively, with staff errors and actions coming in at 24%. The statistics from Baker Hostetler are based on breaches that the company assisted in managing, which totaled over 300 events.

2.3.2.1 Cybercrime Awareness

A complicated worldwide phenomenon, cybersecurity poses difficult socio-technical difficulties to both public and commercial sectors. The bulk of cyberattacks that have been reported can be linked to human mistakes. Studies reveal that one of the most effective preventative measures is to raise users' cybersecurity awareness, despite being both knowledge- and environment-dependent. However, it is difficult to provide complete techniques for improving communication and thwarting cyberattacks due to their ill-defined nature, socio-technical dependencies, ongoing technological advancements, and unclear impact (Khader et al., 2021).

2.3.2.2 Internet Security Practice

Nowadays, individuals are way more concerned about sharing their personal data online than before, according to research (Antón et al., 2010). According to the 2002 survey, information storage, notice, and transfer are the three main concerns for internet users. The study also discovered that there is a disconnect between internet users' privacy concerns and online privacy rules since at the time, these policies placed a strong emphasis on data security and integrity, information gathering, and user choice/consent. Therefore, there was no overlap between the three privacy issues that internet users were most concerned about and the points that internet privacy regulations placed the greatest emphasis on. However, people now seem more willing to speak up against what they see as privacy violations when engaged in online activities. For instance, when Facebook modified its Terms of Service in February 2009 to address its information practices, its users expressed their outrage to the public by starting several Facebook user groups to oppose the change. In response to the uproar, Facebook went back to its old Terms of Service and started rewriting the new ones with less problematic language.

2.3.3 Skill Factor

The knowledge, talent, and experience a person needs to ensure protection from cyberattacks is known as a cybersecurity action skill (CAS) (Ramim, 2015). For instance, action is tailored to a particular computer application each time a user recognizes a well-known one. Even when the same goals are being pursued, an activity is frequently carried out a little bit differently each time. Users can thus manage the appropriate action alternatives to accomplish the same goal. Results are produced by action, which also enables programs to function and bring about events. Maintaining basic antivirus software, availing security updates, to complying with regular safekeeping practices are a few examples of acts in the context of cybersecurity. Therefore, users' CAS is crucial for a successful cybersecurity outcome (Levy & Hovav, 2013).

2.3.3.1 Cyber Crime Frequency

The most recent security risk facing society now is cybercrime, which is unique from all other threats (Friend et al., 2020). Computers, phones, cell phones, and other technological tools are used in cybercrimes to commit crimes like fraud, theft, electronic vandalism, infringement of intellectual property rights, and hacking into computer networks and systems. Information warfare, which comprises war-related actions taken by people, organizations, and governments, is a word associated with cybercrime. Using the same tools and techniques as cybercrimes, these operations are carried out against the computer systems and infrastructure of other businesses and governments (Marshall, 2010). The most problematic threat of the twenty-first century is the cyber threat, which can come from a number of different places, including hackers, terrorists, criminals, insider groups, and foreign countries. It presents difficulties for businesses, governments, and people everywhere. Additionally, while the price of security frameworks is rising, it is gradually becoming more affordable to launch cyberattacks (Gupta & Agarwal, 2017; Duyunov et al., 2021).

2.3.3.2 Cybercrime prevention

Taking situational crime prevention as an example and this technique has been studied the most compared to the other ones they describe. Studies show that antivirus software can recognize and prevent malware attacks, but they are less clear about the effectiveness of warning messages in lowering dangerous hacking. The evidence-based limitations of other security methods, such as firewalls, passwords, and security awareness programs, are far less developed. Campaigns to raise awareness through mass media are useless offline and only partially applicable to illegal activities online. Educational seminars may have value, even though using them in the cyber world will require a different strategy. Even successful mentoring programs may be hampered by the challenges of finding the right populations of offenders and volunteers to help them.

2.4 Characteristics of Generation Z

The youth and adult years of generation z will be witnessing a paradigm shift in both social and economic facets (Sidorcuka & Chesnovicka, 2017). Generation Z will be the millennials' future coworkers. Gen-Zers and millennials share a lot of similarities in terms of visual characteristics, but they also appear to be very different from one another in terms of privacy. The millennial generation benefits from the combined knowledge and skills of generation Z, whereas generation Z approaches cybersecurity obligations with far more unpreparedness. The literature on Generation Z mentions that they want to venture into the professional arena with ease. They find it challenging to imagine developing their professional careers over the long term by taking baby steps. Due to their mobility and fluency in other languages, these individuals hunt for work not only in their immediate surroundings but also around the world. They don't value job security and are willing to switch jobs frequently in search of variety and an escape from everyday life. They represent the smartest and most advanced generation ever. Self-employment is something that many young people view as a form of professional endeavor, especially because they believe it to be more lucrative and to foster a sense of independence. Generation Z is more likely to take risks and let peer pressure influence their choices. The current generation is one of the most tech-savvy generations because they grew up on the internet and social media. The professional traits of this generation z are yet to be widely discussed in journals and articles, as few might be in their first job, while others are yet to be part of the professional workforce (Dolot, 2018).

3. Methodology

An extensive literature review prepared the secondary data for this research, as well as the base for the survey questionnaire that has been utilized to collect the primary data. This self-awareness study was designed to investigate cyber threat awareness among Generation Z Business graduates of Bangladesh. This chapter provides an in-depth overview of the methodology undertaken to complete this study. The following sections will take you through the data collection methods, data analysis process, and sampling techniques used in this research.

3.1 Data

Researchers approached 545 respondents, aged between 23 to 38, to know about their awareness regarding cyber security, cautiousness towards malware, and frequency of reporting cyberattacks. The number of respondents is students from both public and private university containing 273 respondents from American International University - Bangladesh (AIUB), 60 from University of Dhaka, 53 from BRAC University, 42 from North South University, 33 from United International University, 27 from Jahangirnagar University, 25 from East West University, 17 from Southeast University, 9 from Jagannath University, 7 from Independent University, Bangladesh, 5 from ASA University Bangladesh (ASAUB) and only 3 from Green University of Bangladesh. However, there were no respondents from National University graduates, in Bangladesh. Most of the results of the descriptive analysis were displayed as charts or diagrams.

3.2 Data Collection and Variables

The survey questionnaire has four categories of questions, namely Demographic Information, Cyber Knowledge, Cybersecurity Activities, and Cybercrime Consciousness. The first category collects the demographic information of the respondents, whereas the second category tries to capture the level of knowledge the respondents have regarding the cyber world. The third category tries to accumulate knowledge of the range of activities of the respondents in the internet space, and the last one brings in the cautiousness of the respondents against cybercrime. The questions had multiple-choice answers to choose from.

3.3 Data Sample

The sample of the population was selected by using a convenient sampling technique. Convenience sampling involves choosing individuals who are frequently and easily accessible. Because it is less expensive and more convenient than other sample procedures, convenience sampling is frequently preferred by researchers. Convenience sampling can help researchers overcome many challenges. It is simpler to target known people, for example, friends or family, when they are included in the sample (Taherdoost, 2016).

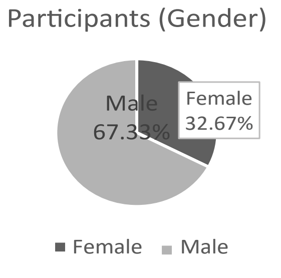
4. Analysis

This section provides an analysis of the questions from the survey questionnaire. The key findings are summarized in graphs and tables in this part. First, we present demographic question [Gender] followed by the sections of security awareness analysis for Internet Usage Frequency, Internet Knowledge Level, Internet Connector and Device Usage, Internet Usage Purpose, Common Operating System, Cyber Crime Frequency, Cybercrime Awareness, Internet Security Practice and lastly cybercrime prevention.

4.1 Demographic Information

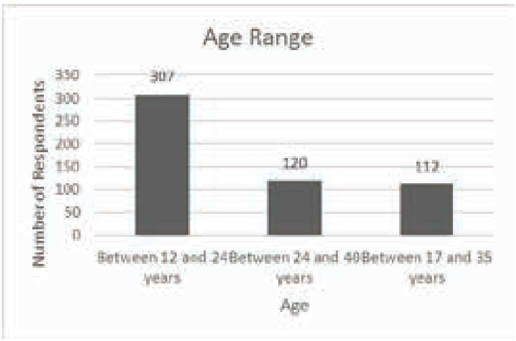
We asked the respondents about their Gender, Age, Level of Education, Major, and Region. Out of the 545 respondents, we got 367 (67%) male and 178 female (33%) [Figure 1] responses. All the respondents fall under the category of generation Z (ages 23 to 40). t of 545, 307 respondents were aged between 12 and 24 years, 120 were between 24 and 40 years and 112 were between 17 and 35 years [Figure 2]. Because there is no proper internet access for Bangladeshi citizens under the age of 12. They are unable to grasp the significance of cybersecurity. Therefore, the responses from these individuals would not be appropriate for this study. Another set of categorical attributes we used was educational level. Where most of the respondents, 372 (68%) have completed their Higher Secondary Certificate exam and the rest of the respondents, 173 (32%) have completed Undergraduate/Postgraduate/PhD [Figure 3]. Respondents were from both outside and inside Dhak

Figure 1:
Gender Distribution of Respondents



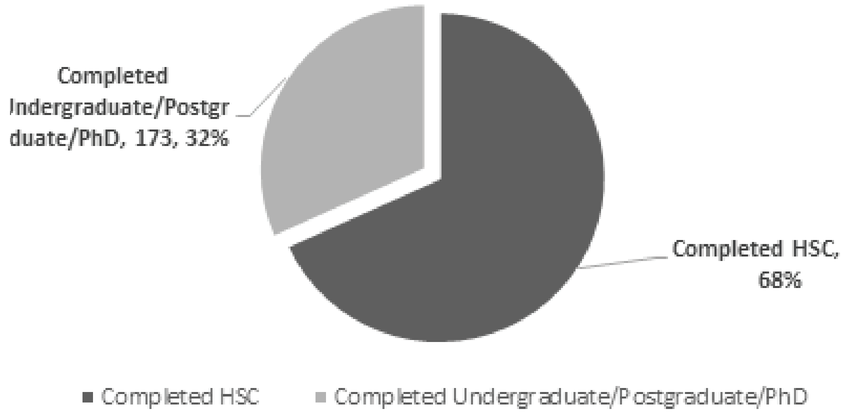
Source: Primary Data from Survey conducted by the researchers

Figure 2:
Age Distribution of Respondents



Source: Primary Data from Survey conducted by the researchers

Figure 3: Level of Education

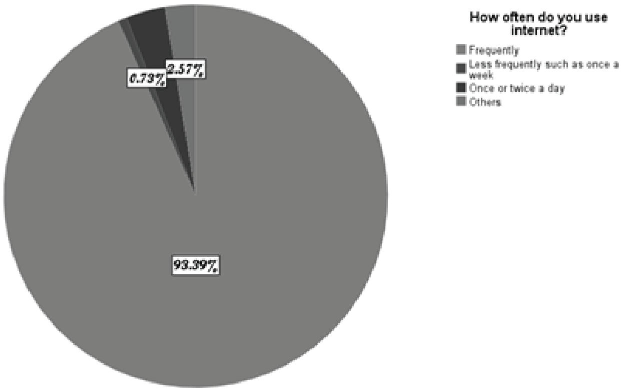


Source : Primary Data from Survey conducted by the researchers

4.2 Information Skills

Initially, the respondents were asked about how often they access the internet. 93.39% said that they access the internet frequently, 2.57% said they access it once or twice a day, with no one accessing the internet just once a week, and 0.73% did not answer the question. The data is pictorially presented in Figure 4. Smartphone and laptop devices were found to be mostly utilized, with a percentage of 35.8% (including when smartphones were selected individually and together with other devices) while others were distributed among desktops and tablets. On the other hand, it was also clear that 110 or 20.2% of the respondents use only smartphones to access the internet. Lastly, we asked about the users operating system of the smartphones where of the users 70.64% were using Android, 28.07% used IOS (Apple), and 1.28% did not answer the question.

Figure 4: Use of Internet

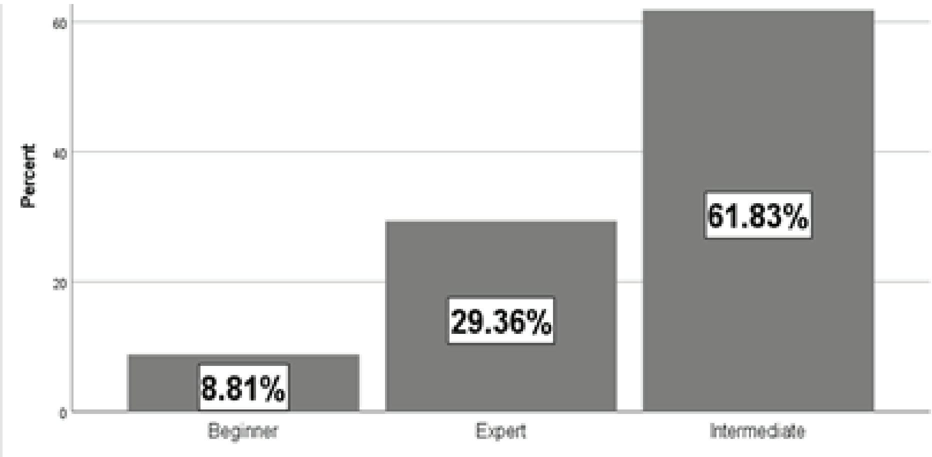


Source: Primary Data from Survey conducted by the researchers

4.3 Cyber Activities

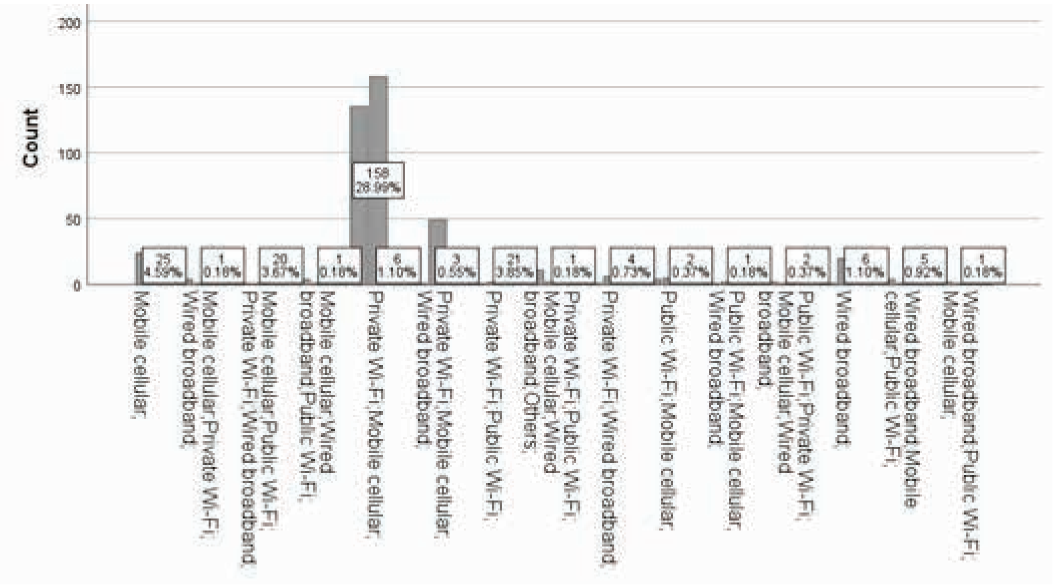
Next, the respondents were asked about their knowledge of the internet or/and how they consider themselves as a user. The answers were distributed to 61.83%, considering themselves as intermediary user, 29.36% as experts, and only 8.81% still in the beginning phase [Figure 5].

Figure 5: Knowledge level on using Internet.



Source: Primary Data from Survey conducted by the researchers

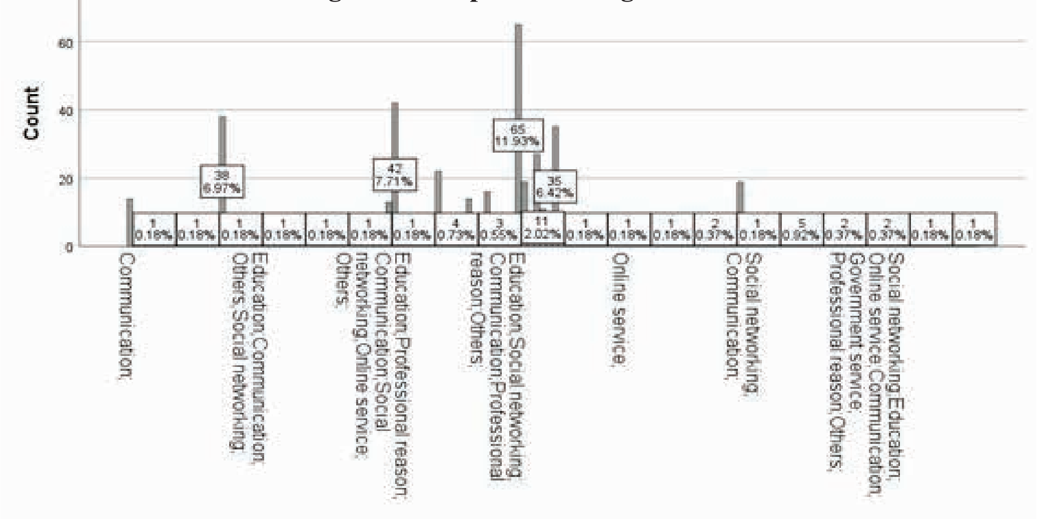
Figure 6: Internet Access via Devices



Source: Primary Data from Survey conducted by the researchers

The bar chart [Figure 6] shows the devices used by Gen-Z of Bangladesh for connecting to the internet. It can be clearly stated that most of the Gen-Z internet users are using private Wi-Fi and mobile cellular for connecting to the internet, where 158 out of 545 (28.99%) are using these methods for using the internet. Next, most of the Gen-Z internet user in Bangladesh is using it for various reasons, but the main reason behind accessing the internet is Education, Social Networking, communication, and online services. Almost 65 (11.93%) out of 545 (100%) are using the internet for these reasons [Figure 7].

Figure 7: Purpose of Using Internet

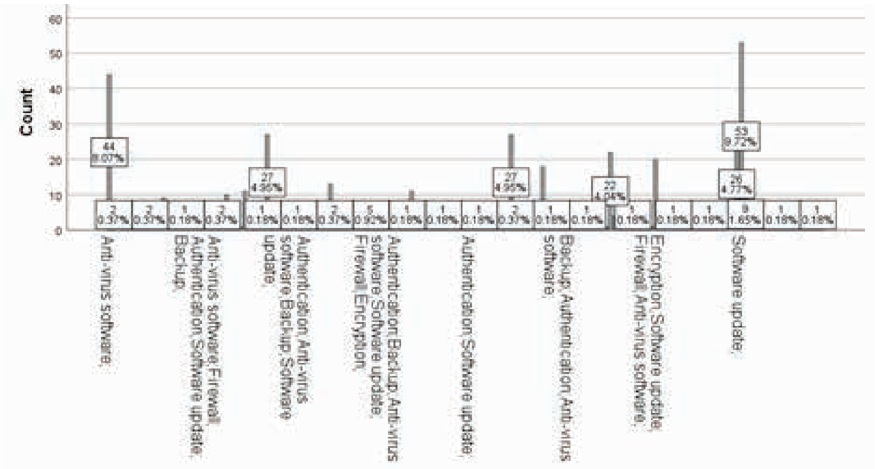


Source: Primary Data from Survey conducted by the researchers

4.4 Security Habits

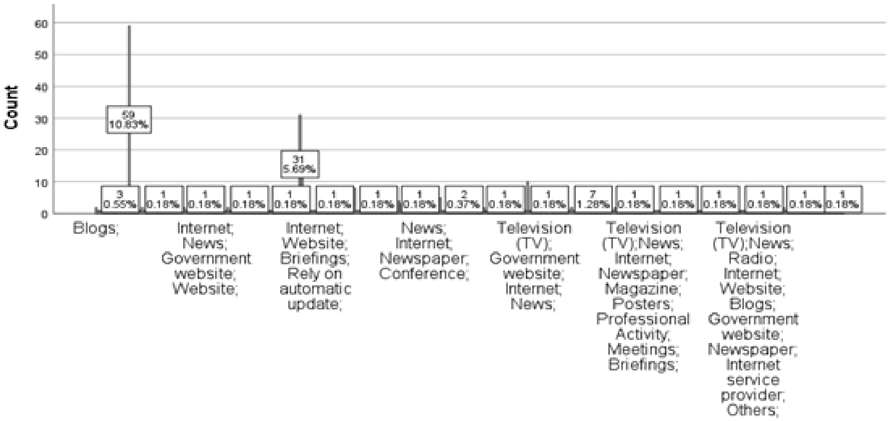
Security habits are very important to access the internet securely and safely. But unfortunately, most people are unaware of using a proper security system for various reasons. In Bangladesh, 53 (9.72%) people out of 545 use only software updates to make their devices protected. On the other hand, 44 people (8.07%) out of 545 use anti-virus software to secure their devices [Figure 8]. This attitude can be attributed to a lack of knowledge about security systems and requirements. According to the graph, 59 (10.83%) people became aware of cyber security from the internet. Similarly, 31 (5.69%) got to know about cybersecurity from the websites, which are accessible by using the internet [Figure 9]. Lastly, in case of reading the terms and conditions [Figure 10] provided by the websites and apps 31.19% sometimes read, while 15.05% of the respondents never read any terms and conditions.

Figure 8: Security Tools and Application



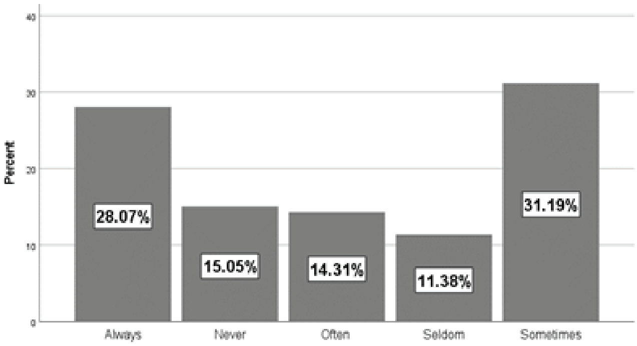
Source: Primary Data from Survey conducted by the researchers

Figure 9: Sources of Awareness of Cybercrimes and Methods of Protection



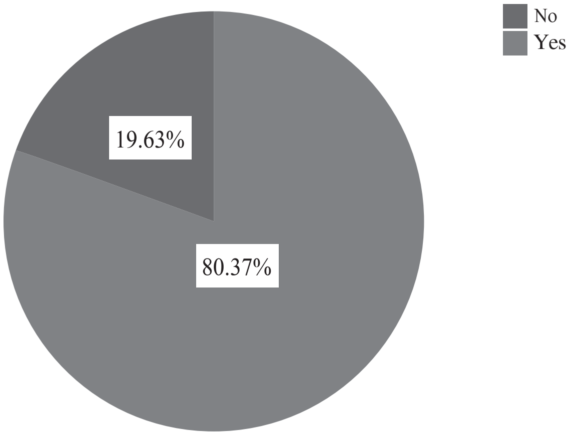
Source: Primary Data from Survey conducted by the researchers

Figure 10: Reading Terms and Conditions



Source: Primary Data from Survey conducted by the researchers

Figure 11: Victim of Cyberattack.



Source: Primary Data from Survey conducted by the researchers

4.5 Victim of Cybercrime

Cyber-attacks are increasing tremendously, and people are getting victimized almost every minute. In the case of generation Z in Bangladesh, out of 545 respondents 80.37% of people have never been attacked, or it might be said they did not have visible proof of attack; but are still on the brink of being attacked. While on the other hand, 19.63% have already been victims of cyber-attacks and are still at risk of being attacked more [Figure 11].

4.6 Possibility of Being a Victim in the Future

Cyber-attacks are no longer a case of "if", but rather "when". But the ratio of reporting those attacks is very low compared to the attacks happening every now and then. Out of 545, only 51 or 9.4% of people report cyberattacks, while the other 90.6% have never reported any cyberattacks [Table 1]. According to a correlation conducted by comparing the ratio of victim of cyberattack with the ratio of reporting the cyber-attack, [Table 2] it is clear that not everyone is reporting those attacks.

Table 1: Reporting Cyberattack

Have you reported the cyberattack?					
		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	**1**	**438**	**80.4**	**80.4**	**80.4**
	No	**56**	**10.3**	**10.3**	**90.6**
	Yes	**51**	**9.4**	**9.4**	**100.0**
	Total	**545**	**100.0**	**100.0**	

Source: Primary Data from Survey conducted by the researchers

Table 2: Co-Relation between Victim of Cyber-Attack and Reporting Cyberattack.

Correlations- Victim of Cyber-Attack VS. Reporting Cyberattack			
		Have you ever been a victim to cyberattack?	Have you reported the cyberattack?
Have you ever been a victim to cyberattack?	Pearson Correlation	1	.936**
	Sig. (2-tailed)		<.001
	N	545	545
Have you reported the cyberattack?	Pearson Correlation	.936**	1
	Sig. (2-tailed)	<.001	
	N	545	545
**. Correlation is significant at the 0.01 level (2-tailed).			

Source: Primary Data from Survey conducted by the researchers

5. Findings

This study is being conducted at a time when Bangladesh has advanced significantly in its cyber activities. The developed nature of Bangladesh's cyber infrastructure requires the creation of cyber security regulations to guard against threats and prevent data loss. Additionally, it is crucial to raise awareness among generation Z because they will be the country's future workforce and will soon be making crucial decisions for many businesses and services. In a context where cyber issues are barely discussed, this paper is making an attempt to examine cyber security awareness. The paper's implications for practice and future research are found in the suggestions made by the authors, including security updates, antivirus software management, compliance with security policies and procedures, making current cybersecurity-related materials needed in tertiary computer studies courses, security awareness training programs, etc.

5.1 Key Contributions

This study makes a significant addition to the field of generation Z's cyber security. This study offers a thorough evaluation of the literature regarding the current situation of generation-cyber z's practice, which is one of its major contributions. This study reveals how generation Z's habits and understanding of cyber dangers are changing, adding to the sparse empirical literature on these topics. It also demonstrates how they are becoming more conscious of cybersecurity-related issues. This study also discusses the significance of cyber security and the reasons why it is crucial for businesses, individuals, and the entire country.

5.2 Limitations and Future Research

This study did not apply any theoretical framework to understand cyber security issues. The findings of the research are derived from the outcomes of a limited sample size consisting of 545 respondents. Additionally, the majority of the comments came from Bangladesh's Dhaka. Therefore, in order to generalize the results to generation Z, future research investigations should seek to receive a higher number of responses. However, the researcher should consider following quota sampling in order to have more accurate data.

The goal of proportional quota sampling is to provide a sample that is proportional to the population being investigated in terms of the strata (groups) being studied, such as the ratio of male to female graduates (Sharma, 2017). The implications of cyber security among generation Z could be better understood by combining the quantitative survey-based method with expert opinion or qualitative interviews.

6. Conclusion

Cyberattacks are more common and provide a serious threat to both people and companies in the modern digital age. To stop cyberattacks and data breaches, university students must be made more aware of cybersecurity issues. According to the study's findings, university students don't seem to be particularly conscious of cybersecurity issues. The findings of several research on student attitudes and understanding of cybersecurity reveal that students are not particularly knowledgeable about how to safeguard their data from cyberattacks. Raising university students' understanding of cybersecurity issues is a continual effort that calls for an all-encompassing strategy (Raju et al., 2022). Universities can strengthen their cybersecurity posture and defend themselves from potential threats by integrating cybersecurity awareness training into the curriculum, educating teachers, staff, and students, conducting regular security training, developing a thorough security policy, encouraging reporting of security incidents, and hiring cybersecurity professionals. The study on cybersecurity awareness among business graduates in Bangladesh can assist the country realize its sustainability objectives (Al Mamun et al., 2021). The research can pinpoint the difficulties and causes influencing cybercrime, examine online behavior, and offer suggestions and strategies for improving cybersecurity policies and practices. The study can also assist the government in correctly implementing ICT rules for a smooth operation of e-commerce company in Bangladesh and attaining the goals of digital Bangladesh given the rising trust in e-commerce facilities and online purchasing Business graduates can help the nation create a safer and more effective online environment, which is crucial for accomplishing sustainability objectives.

References

1. Al Mamun, A., Ibrahim, J. Bin & Mostofa, S. M. (2021). Cyber Security Awareness in Bangladesh: An Overview of Challenges and Strategies. *Int. J. Comp. Sci. Informat. Technol. Res. 9, 88–94.*
2. Alam, T. (2018). A Reliable Framework for Communication in Internet of Smart Devices using IEEE 802.15.4. *ARPN Journal of Engineering and Applied Sciences. 13(10).*
3. Alansari, M. M. H., Aljazzaf, Z. M. & Sarfraz, M. (2019). *On Cyber Crimes and Cyber Security. 1–41.*
4. Alharbi, T. & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing. 5(2), 23.*
5. Alotaibi\, F., Furnell, S., Stengel, I. & Papadaki, M. (2016). *A Survey of Cyber-Security Awareness in Saudi Arabia.*
6. Aloul, F. A. (2012). The Need for Effective Information Security Awareness. *Journal of Advances in Information Technology. 3(3).*

7. Antón, A. I., Earp, J. B. & Young, J. D. (2010). How internet users' privacy concerns have evolved since 2002. *IEEE Security & Privacy. 8(1), 21–27.*

8. Anderson, E. L., Steen, E. & Stavropoulos, V. (2017). Internet use and Problematic Internet Use: a systematic review of longitudinal research trends in adolescence and emergent adulthood. *International Journal of Adolescence and Youth. 22(4), 430–454.*

9. Broadhurst, R. G., Alazab, M. & Chon, S. (2014). Organizations and cybercrime: An analysis of the nature of groups engaged in cybercrime Network Traffic Analysis View project Springer Book: Machine Intelligence and Big Data Analytics for Cybersecurity applications View project. *Article in International Journal of Cyber Criminology.*

10. Chen, Y., Xu, R., Blasch, E. & Chen, G. (2018). *A federated capability-based access control mechanism for Internet of Things (IoTs). 29.*

11. Craigen, D., Diakun-Thibault, N. & Purse, R. (2014). *Technology Innovation Manage ment Review Defining Cybersecurity.*

12. Chowdhury, S., Rahman, M., Doddanavar, I. A., Zayed N. M., Nitsenko, V., Melnykovych, O. & Holik, O. (2023). Impact of Social Media on Knowledge of the COVID-19 Pandemic on Bangladeshi University Students. *Computation. 11(2), 38.*

13. Dangmei, J., Singh, A. & Professor, A. (2016). Understanding the Generation Z: The Future Workforce. *South-Asian Journal of Multidisciplinary Studies (SAJMS). 3.*

14. De Bruijn, H. & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly. 34(1), 1–7.*

15. Diakun-Thibault, N., Craigen, D. & Purse, R. (2014). *Defining Cybersecurity Cybersecurity View project Blockchain and Space Security View project Technology Innovation Management Review Defining Cybersecurity.*

16. Dolot, A. (2018). The characteristics of Generation Z. *E-Mentor. 74, 44–50.*

17. Duyunov, V. K., Zakomoldin, R. V. & Zayed, N. M. (2021). On the concept of positive criminal responsibility in the context of criminal law impact: a critical view. *Journal of Legal, Ethical and Regulatory Issues. 24(SI1), 1-8.*

18. Friend, C., Grieve, L. B., Kavanagh, J. & Palace, M. (2020). Fighting Cybercrime: A Review of the Irish Experience. *International Journal of Cyber Criminology. 14(2), 383–399.*

19. Fedotova, Y. G., Vasilyevich, A. N., Dmitrievna, D. Z., Oxana, V. N., Irina, K. & Zayed, N. M. (2021). Empirical analysis of the role of patriotic education on common strategic- national and economic policy in the modern world: a case study of Russia. *Academy of Strategic Management Journal. 20(SI1), 1-5.*

20. Gupta, R. & Agarwal, S. P. (2017). A comparative study of cyber threats in emerging economies. *Globus: An International Journal of Management & IT. 8(2), 24–28.*

21. Hossain, M. I., Iqbal, M. M. & Zayed, N. M. (2016). The Depressed Higher Education in Bangladesh: Issues and Prospects. *Journal of Thai Interdisciplinary Research. 2559, 140-146.*

22. Hossain, M. I., Hassan, M. M. & Zayed, N. M. (2015). Analyzing Usage Pattern of

Social Networking Sites (SNSs): A Study on SNS Users in Bangladesh. *Stamford Journal of Business Studies. 6/7(2/1), 14-31.*

23. Hassan, T., Alam, M. M., Wahab, A. & Hawlader, M. D. (2020). Prevalence and associated factors of internet addiction among young adults in Bangladesh. *Journal of the Egyptian Public Health Association. 95(1).*
24. Iqbal, M. M., Islam, K. M. A., Zayed, N. M., Beg, T. H., & Shahi, S. K. (2021). Impact of Artificial Intelligence and Digital Economy on Industrial Revolution 4: Evidence from Bangladesh. *American Finance & Banking Review. 6(1), 42-55.*
25. Khader, M., Karam, M. & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information (Switzerland). 12(10).*
26. Khan, S., Shahriar, M. S., Jahan, S. & Zayed, N. M. (2020). The Challenges of Students from Rural Backgrounds in Urban Institutions for Tertiary Education: A Case Study on Students' Migration to Dhaka City. *International Journal of Management (IJM). 11(5), 1225-1231.*
27. Lamba, A., Singh, S. & Singh, B. (2016). Mitigating zero-day attacks in IoT using a strategic framework. *International Journal for Technological Research in Engineering. 4(1).*
28. Levy, Y. & Hovav, A. (2013). *The Role of User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills Influence on Computer Misuse Development of a Cybersecurity Skills Index: A Scenarios-Based, Hands-On Measure of Non-IT Professionals' Cybersecurity Skills View project Social Engineering Exposure View project.*
29. Mustafa, J., Zayed, N. M. & Islam, S. (2018). Students' Perception towards their Teachers' Behaviour: A Case Study on the Undergraduate Students of Daffodil International University, Dhaka, Bangladesh. *International Journal of Development Research (IJDR). 8(10), 23387-23392.*
30. Macdonald, E. K. & Uncles, M. D. (2007). Consumer savvy: conceptualisation and measurement. *Journal of Marketing Management. 23(5–6), 497–517.*
31. Mamun, M. A. A., Zayed, N. M. & Hossain, S. (2013). Using Porter's Diamond to Determine the Condition of ICT in a Developing Country: A Study on Bangladesh. *International Journal of Business & Management Review (IJBMR). 1(3), 138-150.*
32. Marshall, S. M. (2010). Offensive Cyber Capability: *Can it Reduce Cyberterrorism?*
33. Mia, M.M., Zayed, N.M., Islam, K.M.A., Nitsenko, V., Matusevych, T.&, Mordous, I. (2022). *The Strategy of Factors Influencing Learning Satisfaction Explored by First and Second-Order Structural Equation Modeling (SEM). Inventions. 7(3), 59.*
34. Nowrin, S. & Bawden, D. (2018). Information security behaviour of smartphone users: An empirical study on the students of university of Dhaka, Bangladesh. *Information and Learning Science. 119(7–8), 444–455.*
35. Nahar, S., Hasan, K. B. M. R., Chowdhury, T. S., Khan, S. & Zayed, N. M. (2020). Business Students' Attitude towards Internet Usage: A Strategic Analysis on the Students of University of Rajshahi, Bangladesh. *Academy of Strategic Management Journal (ASMJ). 19(1), 1-6.*

36. Rahim, N. H. A., Hamid, S., Kiah, L. M., Shamshirband, S. & Furnell, S. (2015). *A systematic review of approaches to assessing cybersecurity awareness. Kybernetes. 44(4), 606–622.*

37. Raju, R., Abd Rahman, N. H. & Ahmad, A. (2022). Cyber Security Awareness in Using Digital Platforms among Students in a Higher Learning Institution. *Asian Journal of University Education. 18(3), 756–766.*

38. Ramim, Y. M. (2015). An assessment of competency-based simulations on e-learners' manage-ment skills enhancements. *Interdisciplinary Journal of e-Skills and Lifelong Learning. 11.*

39. Ray, P. P. (2016). A survey of IoT cloud platforms. *Future Computing and Informatics Journal. 1(1–2), 35–46.*

40. Sharma, G. (2017). *IJAR. 3(7), 749–752.*

41. Shehab, A., Marni, N., Hamed, K. S. S. A., bin Marni, D. & Shehab, A. A. A. (2020). Evidence In Cybercrimes: A Comparative Study Between Islamic Law and UAE Legislations *Ejaculatory Hood Sparing Prostatectomy View Project. Journal of Critical Reviews.*

42. Shukla, S. S., Tiwari, M. M., Lokhande, A. C., Tiwari, T., Singh, R. & Beri, A. (2022). A Comparative Study of Cyber Security Awareness, Competence and Behavior. *2022 5th International Conference on Contemporary Computing and Informatics(IC3I). 1704–1709.*

43. Sidorcuka, I. & Chesnovicka, A. (2017). *Methods of attraction and retention of generation z staff. CBU International Conference Proceedings. 5, 807–814.*

44. Singh, A. P. (2017). A Study on Zero Day Malware Attack. *IJARCCE. 6(1), 391–392.*

45. Taherdoost, H. (2016). Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. *International Journal of Academic Research in Management (IJARM). 5(2).*

46. Ten, C. W., Liu, C. C. & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems. 23(4), 1836–1846.*

47. Vladimirovna, N. E. & Zayed, N. M. (2021). Digital industrialization: entrepreneurial features of advanced nations' innovation policies during industrial revolution 4.0. *Academy of Entrepreneurship Journal. 27(6), 1- 8.*

48. Wang, K., Guo, X. & Yang, D. (2022). Research on the Effectiveness of Cyber Security Awareness in ICS Risk Assessment Frameworks. *Electronics. 11(10), 1659.*

49. Wei, L. & Zhang, M. (2008). *The impact of Internet knowledge on college students' intention to continue to use the Internet. 3.*

50. Whitman, M. E., Zafar, H. & Machinery, A. C. (2012). Special Interest Group on Man agement Information Systems. (2012). *InfoSec CD '12*: proceedings of the 2012 Information Security Curriculum Development Annual Conference, 2012, Kennesaw, GA. ACM.*

51. Witkowski, K. (2017). Internet of Things, Big Data, Industry 4.0 - Innovative Solutions in Logistics and Supply Chains Management. *Procedia Engineering. 182, 763–769.*

52. Zhaltyrbayeva, R., Shalkharov, Y. S., Bitemirov, K. T., Ismailova, B. S., Kurmanova, A. K., Berdibaev, Y. M. & Zayed, N. M. (2021). The legal status of the designation of artificial intelligence in a system of modern law. *Journal of Legal, Ethical and Regulatory Issues. 24(4), 1-8.*

Appendix

Questionnaire

01. What is your gender?
    - Male
    - Female
02. What is the age?
    - Between 12 and 24 years
    - Between 24 and 40 years
    - Older than 40
03. What is the Level of education?
    - Completed Undergraduate/Postgraduate/PhD
    - Completed HSC
    - Not completed HSC
04. What is your Majors?
    - Computer Science
    - Education
    - Medicine and Public Health
    - Engineering
    - Business Studies
    - Arts
    - Others
05. What is the Region?
    - Dhaka
    - Outside Dhaka
06. How often do you use the internet?
    - Frequently
    - Once or twice a day
    - Once a week
    - Others
07. What type of device do you use to access the internet?
    - Smartphone
    - Desktop
    - Laptop
    - Tablet
08. How would you classify your knowledge level on using internet?
    - Beginner
    - Intermediate
    - Expert

09. How do you connect with the internet?
    - Wi-Fi
    - Mobile data
    - Local ISP broadband
    - Others

10. The purpose for which I access the internet:
    - Studies
    - Social Network like Facebook
    - Online service
    - Communication
    - Government service
    - Professional reason
    - Others

11. What operating system do you use on your smartphones?
    - IOS (Apple)
    - Android
    - Prefer not to say

12. Security tools and applications that you use for your devices:
    - Authentication
    - Backup
    - Anti-virus software
    - Firewall
    - Software update
    - Encryption
    - None

13. Which device do you use your security tools on?
    - Desktop
    - Laptop
    - Smartphone
    - Tablet

14. Do you update your security software?
    - Yes, I manually update
    - It gets updated automatically

15. From which source you became aware of cybercrimes and methods to protect yourself from them?
    - Television (TV)
    - News
    - Radio
    - Internet
    - Website
    - Email bulletins
    - Blogs
    - Government website

- Internet service provider
- Rely on automatic update
- Newspaper
- Magazine
- Posters
- Professional Activity
- Conference
- Meetings
- Briefings
- Government or professional report
- I do not feel that I keep myself updated
- Others

16. Who do you think should be responsible for raising awareness
    - Government
    - The media
    - Internet services
    - User
    - Education system

17. Have you ever been a victim of a cyberattack?
    - Yes
    - No