Building Cybersecurity Awareness among Gen Z University Students: The Mediating Role of Self-Efficacy

by

Arjun Sutradhar
ID: CSE2101022038

Md. Ashraful Islam Tarek
ID: CSE2001019081

Md. Ashak-Ul-Islam
ID: CSE2101022065

Supervised by
Professor Bulbul Ahamed

Submitted in partial fulfillment of the requirements for the degree of
Bachelor of Science in Computer Science and Engineering



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SONARGAON UNIVERSITY (SU)
January 2025

APPROVAL

The thesis titled "**Building Cybersecurity Awareness among Gen Z University Students: The Mediating Role of Self-Efficacy**" submitted by Arjun Sutradhar (CSE2101022038), Md. Ashraful Islam Tarek (CSE2001019081) and Md. Ashak-Ul-Islam (CSE2101022065) to the Department of Computer Science and Engineering, Sonargaon University (SU), has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Engineering and approved as to its style and contents.

Board of Examiners

Prof. Bulbul Ahamed — **Supervisor**
Head,
Department of Computer Science and Engineering
Sonargaon University (SU)

(Examiner Name and Signature) — **Examiner 1**
Department of Computer Science and Engineering
Sonargaon University (SU)

(Examiner Name and Signature) — **Examiner 2**
Department of Computer Science and Engineering
Sonargaon University (SU)

(Examiner Name and Signature) — **Examiner 3**
Department of Computer Science and Engineering
Sonargaon University (SU)

DECLARATION

We, hereby, declare that the work presented in this thesis is the outcome of the investigation performed by us under the kind supervision of **Professor Bulbul Ahamed** and **Head,** Department of Computer Science and Engineering, Sonargaon University, Dhaka, Bangladesh. We reaffirm that no part of this thesis has been or is being submitted elsewhere for the award of any degree or diploma.

Countersigned

(Prof. Bulbul Ahamed)
Supervisor

Signature

Arjun Sutradhar
ID: CSE2101022038

Md. Ashraful Islam Tarek
ID: CSE2001019081

Md. Ashak-Ul-Islam
ID: CSE2101022065

ABSTRACT

The rapid advancement of digital technology has brought cybersecurity to the forefront of global concerns, particularly as online platforms become essential for education and work. This shift from offline to online environments increases risks to privacy and data protection, creating pressing challenges for Gen Z university students in Bangladesh who rely heavily on internet-based learning. This study investigates the influence of cybersecurity knowledge, password security, and social networking on cybersecurity awareness among Bangladeshi Gen Z university students, with a focus on the mediating role of self-efficacy. Data were collected from 430 Gen Z students across five private universities in Bangladesh, using a stratified random sampling method in a cross-sectional study design. A positivist approach and hypothetical-deductive method were employed, with validated scales adapted from previous studies to measure the constructs. Data analysis was performed using Smart PLS-SEM 4.0. The findings reveal significant positive associations between cybersecurity knowledge and password security with cybersecurity awareness, though no significant relationship was observed between social networking and cybersecurity awareness. Additionally, self-efficacy was found to mediate the relationships between cybersecurity knowledge, password security, and social networking with cybersecurity awareness. The study underscores the critical need to improve cybersecurity literacy and responsible internet use among university students. This research contributes to the literature by highlighting the importance of self-efficacy in fostering effective cybersecurity behaviors within an academic setting.

Keywords: Gen Z, cybersecurity awareness, cybersecurity knowledge, password security, self-efficacy, Bangladesh

ACKNOWLEDGMENT

At the very beginning, we would like to express my deepest gratitude to the Almighty God for giving us the ability and the strength to finish the task successfully within the schedule time.

We are auspicious that we had the kind association as well as supervision of **Professor Bulbul Ahamed**, and Head, Department of Computer Science and Engineering, Sonargaon University whose hearted and valuable support with best concern and direction acted as necessary recourse to carry out our thesis.

We extend our sincere thanks to **Dr. Mohammad Rashed Hasan Polas,** Lecturer and Researcher, Department of Business Administration, Sonargaon University, for his encouragement, assistance, and thoughtful advice, which significantly contributed to the successful completion of this work.

We are also thankful to all our teachers during our whole education, for exposing us to the beauty of learning.

Finally, our deepest gratitude and love go to our parents for their support, encouragement, and endless love, which have always been our greatest source of strength.

LIST OF ABBREVIATIONS

ACM	Association for Computing Machinery
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
CA	Cybersecurity Awareness
CK	Cybersecurity Knowledge
Gen Z	Generation Z
H1, H2, H3, H4, H5, H6	Hypotheses (1, 2, 3, 4, 5, 6)
ICT	Information and Communication Technology
PLS-SEM	Partial Least Squares Structural Equation Modeling
PS	Password Security
SE	Self-Efficacy
SEM	Structural Equation Modeling
SN	Social Networking
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege

TABLE OF CONTENTS

Title			Page No.
DECLARATION …….……..			iii
ABSTRACT ……...…….			iv
ACKNOWLEDGEMENT ……..……			v
LIST OF ABBREVIATION ……..…….			vi
CHAPTER 1			1 – 17
INTRODUCTION			
1.1	Introduction ……..…..…….…….....		1 – 2
1.2	Background of the Study …….…....……..		2
1.3	Problem Statement …….....…….….....		2 – 3
1.4	Objectives of the Study …….....….….....		3 – 5
1.5	Research Questions…….....…….....		5 – 8
1.6	Significance of the Study…….... ..……..		8 – 9
1.7	Scope of the Study…….....…….….....		10 – 12
	1.7.1	Demographic Scope…….	10
	1.7.2	Thematic Scope……	10 – 11
	1.7.3	Geographical Scope……	11
	1.7.4	Theoretical Scope……	11 – 12
	1.7.5	Practical Scope……	12
1.8	Operational Definitions…….....…….….....		12 – 13
1.9	Organization of the Thesis……...…....…..…		14 – 15
1.10	Summary of the Chapter…….....……		16 – 17
CHAPTER 2			18 – 31
LITERATURE REVIEW			
2.1	Introduction ……		18
2.2	Cybersecurity Awareness ……. …….....		18 – 19
2.3	Cybersecurity Challenges Among Gen Z...…….……...		19 – 20
2.4	Self-Efficacy and Behavioral Outcomes.....		20

2.5 The Role of Theories in Cybersecurity Awareness..... 20
2.6 Hypotheses Development …….. 21 – 30
2.6.1 Cybersecurity Knowledge on Cybersecurity Awareness …. 21– 23
2.6.2 Perceived Security on Cybersecurity Awareness ……. 24 – 26
2.6.3 Social Networking on Cybersecurity Awareness ……. 26 – 28
2.6.4 The Mediating Role of Sefl-Efficacy ……... 28 – 30
2.7 Conceptual Framework ……. 31

CHAPTER 3 32 – 48
RESEARCH METHODOLOGY
3.1 Introduction ……... 32
3.2 Research Design…….....……..……..... 33
3.3 Sample Size Determination.....…….…….... 34
3.4 Sampling Technique..... 35 – 37
3.4.1 Stratified Random Sampling..... 35
3.4.2 Random Selection within Strata..... 35 – 36
3.4.3 Stratified Random Sampling Breakdown..... 36 – 37
3.5 Data Collection Methods..... 37 – 39
3.5.1 Primary Data Collection..... 37 – 38
3.5.2 Data Collection Process..... 38
3.5.3 Challenges and Mitigation..... 39
3.6 Research Instrument..... 40 – 41
3.7 Variables and Measures..... 42 – 44
3.8 Data Analysis Techniques..... 44 – 46
3.9 Limitations of the Methodology..... 46 – 47
3.10 Recommendations..... 48

CHAPTER 4 49 – 55
DATA ANALYSIS AND FINDINGS
4.1 Descriptive Analysis of Respondents ……... 49
4.2 Measurement, Validity and Reliability..... 49 – 52
4.3 Hypotheses Testing Outcomes..... 53

4.4 Structural Equation Modeling (SEM) Results..... 54 –55

4.4.1 Indirect Effects: Mediating Role of Self-Efficacy..... 54 –55

4.4.1 Summary of SEM Results..... 55

CHAPTER 5 56 – 70

DISCUSSION AND CONCLUSION

5.1 Implications of the Study ……. 56

5.2 Theoretical Contributions ……..... 57

5.3 Practical Implications for University Administrators …….. 57 – 60

5.3.1 Cybersecurity Training Programs..... 57 – 58

5.3.2 Integration into Curriculum..... 58

5.3.3 Building Self-Efficacy..... 58

5.3.4 Promoting Responsible Social Networking..... 58

5.3.5 Policy Development and Enforcement..... 58

5.3.6 Collaboration with Cybersecurity Experts..... 58

5.3.7 Awareness through Technology..... 58 – 59

5.3.8 Supporting Vulnerable Groups..... 59

5.4.1 Building Confidence in Cybersecurity Practices..... 59

5.4.2 Self-Efficacy as a Mediator..... 59 – 60

5.4.3 Impact of Self-Efficacy on Cybersecurity Awareness..... 60

5.4.4 Educational Implications..... 60

5.5 Comparative Analysis with Global Findings..... 60 – 62

5.5.1 Cybersecurity Knowledge and Awareness..... 60 – 61

5.5.2 Password Security as a Key Predictor..... 61

5.5.3 Role of Social Networking in Cybersecurity Awareness..... 61 – 62

5.5.4 Mediating Role of Self-Efficacy..... 62

5.5.5 Implications for Global Cybersecurity Education..... 62

5.6 Policy Recommendations for Cybersecurity Education..... 62 – 64

5.6.1 Integrating Cybersecurity Education into University Curricula..... 63

5.6.2 Fostering Self-Efficacy through Practical Training..... 63

5.6.3 Increasing Public Awareness Campaigns..... 63
5.6.4 Emphasizing Password Security and Best Practices..... 64
5.6.5 Promoting Digital Literacy and Critical Thinking..... 64
5.7 Limitations of the Study..... 64 – 66
5.7.1 Sample Limitation..... 64
5.7.2 Cross-Sectional Design..... 65
5.7.3 Self-Reported Data..... 65
5.7.4 Limited Focus on External Factors..... 65
5.7.5 Generalizability to Other Contexts..... 65 – 66
5.7.6 The Role of Other Psychological Factors..... 66
5.8 Directions for Future Research……..... 66 – 67
5.8.1 Longitudinal Studies to Assess Causal Relationships..... 66
5.8.2 Expansion of the Sample Population..... 66
5.8.3 Exploring the Role of Other Psychological Factors..... 67
5.8.4 In-Depth Exploration of Social Networking's Impact..... 67
5.8.5 Investigating Cybersecurity Behaviors Beyond Awareness 67
5.9 Significance of Cybersecurity Literacy in Gen Z s …… 67 – 69
5.9.1 Protection Against Cyber Threats..... 68
5.9.2 Promoting Responsible Online Behavior..... 68
5.9.3 Enhancing Self-Efficacy in Cybersecurity Practices..... 68
5.9.4 Mitigating the Digital Divide..... 68 – 69
5.9.5 Facilitating Safer Online Education..... 69
5.10 Conclusion: Bridging Knowledge and Practice in Cybersecurity….. 69 - 70

REFERENCES …… 71 – 72
APPENDIX …… 73 – 77

LIST OF TABLES

Table No.	Title	Page No.
Table 2.1	Summary of Hypothesis with Previous Studies	30
Table 3.1	Respondents Profile	36
Table 3.2	Challenges and Mitigation	39
Table 3.3	Independent Variables	42
Table 3.4	Dependent Variables	43
Table 3.5	Mediating Variable	43
Table 4.1	Measurement of Model Assessment	50
Table 4.2	Values of the Stone Geisser indicator (Q2) and Cohen's indicator (f2) of the model in the SEM	51
Table 4.3	Fornell-Larcker criterion Analysis for discriminant validity	51
Table 4.4	The heterotrait-monotrait (HTMT) analysis for discriminant validity	52
Table 4.5	Direct and Indirect Effects Hypothesis	53

LIST OF FIGURES

Figure No.	Title	Page No.
Fig.2.1	Conceptual Framework	31

CHAPTER ONE

INTRODUCTION

1.1 Introduction

In today's rapidly evolving digital age, how we interact with the world has changed dramatically. This transformation is even more profound for Generation Z (Gen Z), often described as the most connected demographic in history (Ali & Ahmed, 2022). Born between 1997 and early 2012, Gen Z is the first generation to grow up with constant access to the internet and digital devices, shaping how they learn, communicate, and navigate daily life (Hernandez-Arriaza et al., 2023). For Gen Z students, digital platforms are indispensable. These technologies, from e-learning tools and virtual classrooms to social media and online banking, play a central role in their education, social interactions, and everyday activities (Andoh & Owusu, 2023; Polas et al., 2024; Chen & Ma, 2023). In Bangladesh, this dependency on digital platforms is especially evident as more students turn to online resources for education, entertainment, and convenience (Chen & Ma, 2023).

While these platforms offer countless opportunities, they also introduce significant challenges. A growing reliance on digital tools requires users to develop strong digital literacy and remain vigilant about online safety (Cheng & Zhang, 2023). Unfortunately, many Gen Z students in Bangladesh are vulnerable to specific cybersecurity threats such as phishing attacks, identity theft, malware, and data breaches. For instance, a student might fall victim to a phishing attack when they receive a fake email claiming to be from their school, asking for their login credentials. The lack of awareness or training to recognize and counter these risks further heightens this vulnerability (Li & Liu, 2024). The situation in Bangladesh is very worrying. Many students do not know how to stay safe online because they do not have access to cybersecurity education or resources (Ahamed et al., 2024). Digital literacy programs are not widely available, which increases the risk of online threats. It makes it urgent to act quickly and take steps to protect students in the digital world.

To tackle these challenges, we need to help students understand cybersecurity better. Educational programs and awareness campaigns should teach simple but important practices, like spotting phishing scams, making strong passwords, and protecting their

privacy online. (Li & Tang, 2023; Wang & Li, 2023). By fostering a proactive approach to cybersecurity, students can safeguard their digital presence and feel empowered to contribute to a safer online community for their peers (Xie & Zhang, 2021).

1.2 Background of the Study

In today's digital world- technology has brought many benefits and created cybersecurity challenges. As more students rely on the Internet for education, communication, and everyday tasks, they are becoming increasingly vulnerable to online threats like hacking, identity theft, data breaches, and privacy issues. Research shows that many students lack enough cybersecurity knowledge or skills to stay safe online. Limited access to cybersecurity education and awareness programs leaves them unprepared to handle online risks effectively (Zhou & Zhang, 2024). Additionally, as cyber threats become more advanced, students often lack the confidence to protect themselves, which makes them more susceptible to attacks.

Self-efficacy and Student's confidence in their ability to secure themselves online significantly improve cybersecurity awareness. However, current efforts mainly focus on providing information without helping students build the confidence to apply this knowledge in real-life situations (Zhang & Zhu, 2023). This study explores how cybersecurity knowledge, password security, social networking, and self-efficacy affect cybersecurity awareness. By understanding these factors, the research seeks to offer valuable insights into enhancing cybersecurity education for university students in Bangladesh.

1.3 Problem Statement

University students in Bangladesh, especially those from Gen Z, use online platforms more than ever for their studies, socializing, and daily tasks. However, this growing reliance on the internet makes them easy targets for cyber threats like hacking, phishing, and data breaches (Zhou & Zhang, 2024). Many students do not know enough about staying safe online and often do not follow basic security practices, increasing the chances of their personal information being stolen or misused (Xu & Li, 2022). As online threats become more advanced, young people are at greater risk. Cybercriminals often take advantage of students who do not know how to protect themselves, leading to serious problems like identity theft, financial fraud, or loss of private data. This makes it very

important to teach students how to be safer online and prioritize cybersecurity education (Zhang & Zhu, 2023).

Unfortunately, most programs that teach cybersecurity focus only on giving information. They rarely help students feel confident in using that knowledge in real-life situations. This confidence, known as self-efficacy, is essential because students are more likely to practice safe online habits when they believe they can make a difference. Without it, even students who know the basics may fail to apply them effectively (Zhang & Zhu, 2023; Zhou & Zhang, 2024). For example, students might know they should use strong passwords or avoid suspicious links, but they do not always follow these rules because they are not confident, they can truly protect themselves. This lack of confidence prevents them from taking the steps needed to stay safe online, no matter how much they have learned (Wang & Liu, 2023).

If this problem is not addressed, future generations of students will face even more significant risks. As we rely more on digital tools and cyber-attacks become brighter, the gap between those who can protect themselves and those who cannot will grow. To fix this, we need programs that do more than teach— they must empower students to implement their knowledge. If we fail to take action now, we risk leaving a generation unprepared for the dangers of the online world, which could lead to serious problems for individuals and society.

1.4 Objectives of the Study

The rapid advancement of technology has made cybersecurity awareness a critical issue in today's digital age. This study's objectives address key aspects of how cybersecurity awareness can be influenced and enhanced, focusing on several essential factors and their interplay.

RO1- To investigate the influence of cybersecurity knowledge, password security, and social networking on cybersecurity awareness.

The first objective of this study is to understand the factors that influence cybersecurity awareness. Cybersecurity knowledge is foundational to individuals' ability to recognize threats and implement protective measures in the digital world. This study will analyze how awareness of risks, familiarity with cybersecurity practices, and understanding key

principles impact overall cybersecurity behavior. Similarly, password security is crucial in safeguarding personal and organizational data. This study explores how secure password practices—such as creating strong passwords and multifactor authentication—contribute to enhanced awareness and protection.

Another focus of this objective is the role of social networking platforms. These platforms, while widely used for communication and information sharing, often expose users to potential cybersecurity risks, such as phishing, identity theft, and privacy breaches. This study highlights the opportunities and challenges these platforms present by examining how individuals' interactions and behaviors on social networking sites impact their cybersecurity awareness. Together, these factors—cybersecurity knowledge, password security, and social networking—are integral to developing a comprehensive understanding of what shapes individuals' awareness and practices in cybersecurity.

RO2- To examine the mediating role of self-efficacy in these relationships.

Self-efficacy, an individual's belief in their ability to execute specific actions to achieve desired outcomes, is a crucial psychological factor in adopting and maintaining cybersecurity practices. This study investigates whether self-efficacy mediates the relationship between the factors identified in RO1 and cybersecurity awareness. For example, while cybersecurity knowledge and password security practices are essential, their influence on awareness may be enhanced if individuals feel confident in their ability to understand and apply these measures effectively. Similarly, self-efficacy may determine whether individuals engage in protective behaviors on social networking platforms. Those with higher confidence levels in their cybersecurity skills may be more proactive in identifying risks, avoiding suspicious links, and managing their privacy settings. By examining this mediating role, the study seeks to provide a more nuanced understanding of how self-efficacy contributes to cybersecurity awareness and behavior.

RO3- To contribute to the academic literature and practical initiatives for improving cybersecurity literacy.

The final objective of this study is to make meaningful contributions to academic research and practical applications. The study will address gaps in the existing literature by examining the relationships between cybersecurity knowledge, password security, social networking, and self-efficacy. The findings will provide theoretical insights that can

inform future research and contribute to a growing body of knowledge in cybersecurity. In addition, the study aims to offer actionable recommendations for improving cybersecurity literacy. These insights can guide educational programs, organizational policies, and public awareness campaigns designed to empower individuals with the skills and confidence to navigate the digital landscape securely. This study seeks to enhance collective efforts toward a more secure digital environment by aligning academic and practical goals.

1.5 Research Questions

This study investigates the intricate factors that shape the cybersecurity awareness of Generation Z university students, a cohort uniquely immersed in digital technology from a young age. The following research questions explore the direct and mediated relationships between key variables such as cybersecurity knowledge, password security, social networking behavior, and self-efficacy.

RQ1- To what extent does cybersecurity knowledge influence the cybersecurity awareness of Gen Z university students?

Cybersecurity knowledge serves as the foundation for cultivating awareness of potential threats in digital environments. This research question seeks to explore how familiarity with cybersecurity principles influences the ability of Generation Z university students to identify and mitigate risks. In an era marked by increasing reliance on digital technologies, understanding concepts such as malware, phishing, and secure browsing is essential for maintaining security. The study focuses on examining the depth and breadth of knowledge among Gen Z students, who have grown up with digital tools integrated into their daily lives. Despite this exposure, previous research has indicated varying levels of understanding of cybersecurity concepts within this population. For example, some students may have superficial knowledge of basic security measures, such as avoiding suspicious emails, but lack awareness of more complex threats like zero-day vulnerabilities or sophisticated social engineering attacks.

By assessing the correlation between cybersecurity knowledge and awareness, this research question aims to identify gaps that could hinder students' ability to safeguard their personal and academic data. It also seeks to understand whether formal education in cybersecurity, such as workshops, online courses, or university programs, contributes significantly to heightened awareness. Ultimately, this question sheds light on how

knowledge serves as a stepping stone toward developing proactive and resilient cybersecurity habits.

RQ2- How does password security behavior affect cybersecurity awareness among Gen Z university students?

Password security is a fundamental yet often overlooked component of cybersecurity awareness. This research question investigates how Generation Z university students' password management practices influence their ability to recognize and respond to cybersecurity threats. Password security behaviors include creating strong and unique passwords, updating them regularly, and utilizing password management tools.

Despite widespread awareness campaigns emphasizing the importance of secure passwords, research suggests that many individuals—especially students—continue to engage in risky behaviors, such as reusing passwords across multiple platforms or choosing easily guessable combinations. For Gen Z students, these practices could stem from convenience, a lack of awareness about potential risks, or an underestimation of the consequences of password breaches. This study seeks to explore whether students who follow best practices in password security exhibit higher levels of cybersecurity awareness compared to those who do not. It also considers the role of external factors, such as institutional policies requiring regular password updates or multifactor authentication, in shaping these behaviors. By addressing this question, the study aims to identify actionable insights for improving password security practices among university students. It also explores how secure password habits contribute to broader cybersecurity awareness, fostering a culture of vigilance and responsibility in digital spaces.

RQ3- What is the impact of social networking behavior on the cybersecurity awareness of Gen Z university students?

Social networking platforms are an integral part of Generation Z's daily lives, offering avenues for communication, entertainment, and information sharing. However, these platforms also expose users to various cybersecurity risks, such as phishing, identity theft, and privacy breaches. This research question examines how social networking behaviors influence the cybersecurity awareness of university students. The study focuses on specific behaviors, such as sharing personal information, interacting with unfamiliar users, and engaging with external links. For example, students who frequently share details about their lives on social media may unknowingly provide cybercriminals with

information that can be used in phishing schemes or other malicious activities. Similarly, clicking on unverified links or downloading files from unknown sources can expose users to malware or data breaches.

This research question also explores whether students' awareness of these risks influences their behavior on social networking platforms. For instance, are students who are more aware of cybersecurity threats more cautious in their online interactions? Additionally, the study seeks to identify whether specific educational initiatives or platform-specific features, such as privacy settings or warnings about suspicious links, play a role in shaping safer behaviors. By addressing the interplay between social networking habits and cybersecurity awareness, this question aims to provide insights into how students can navigate digital spaces more securely while enjoying the benefits of social media.

RQ4- How does self-efficacy mediate the relationship between cybersecurity knowledge, password security, and social networking on cybersecurity awareness?

Self-efficacy, or the belief in one's ability to perform specific tasks successfully, is a critical psychological factor that influences cybersecurity behavior. This research question examines whether self-efficacy mediates the relationship between cybersecurity knowledge, password security, and social networking behaviors and their impact on cybersecurity awareness. Students with high self-efficacy are more likely to feel confident in their ability to apply cybersecurity knowledge, adopt secure password practices, and navigate social networking platforms safely. For example, individuals with strong self-efficacy may be more proactive in creating complex passwords, updating them regularly, and using multifactor authentication. Similarly, they may be more cautious and deliberate in their interactions on social media, avoiding risky behaviors and recognizing potential threats.

This study seeks to determine whether self-efficacy enhances the effectiveness of cybersecurity knowledge and behaviors, ultimately contributing to higher levels of awareness. It also explores whether interventions aimed at improving self-efficacy, such as training programs or gamified learning experiences, can amplify the positive impacts of other factors. By addressing this question, the research aims to provide a holistic understanding of the psychological and behavioral dynamics that underpin cybersecurity awareness among Gen Z university students. The findings will offer valuable insights for

designing educational initiatives and intervention strategies that empower students to take control of their digital security confidently.

1.6 Significance of the study

The significance of this study lies in its potential to address a critical gap in the cybersecurity landscape, particularly among Gen Z university students. As digital natives, Gen Z individuals are highly immersed in technology, relying on digital platforms for education, social interaction, and entertainment. However, their familiarity with technology does not necessarily translate into an awareness of the risks associated with its misuse or the measures needed to mitigate such risks. This study, therefore, aims to provide a comprehensive understanding of the factors influencing cybersecurity awareness, emphasizing the role of cybersecurity knowledge, password security, and social networking behaviors. These insights are particularly valuable as cyber threats continue to evolve, becoming more sophisticated and challenging to combat. For this reason, understanding and enhancing cybersecurity awareness among university students is both timely and necessary.

From an academic perspective, this study contributes to the growing body of literature on cybersecurity awareness, offering insights into a demographic that is underrepresented in existing research. While previous studies have explored cybersecurity issues in various populations, few have specifically examined Gen Z university students. Moreover, the introduction of self-efficacy as a mediating variable represents a novel approach to understanding the psychological and behavioral mechanisms underpinning cybersecurity practices. Self-efficacy, which reflects individuals' confidence in their ability to perform tasks effectively, has been widely studied in various disciplines but remains underexplored in the context of cybersecurity. By addressing this gap, the study not only expands theoretical frameworks but also opens avenues for future research on the interplay between individual psychological factors and cybersecurity behaviors. On a practical level, the findings of this study have significant implications for educators, policymakers, and university administrators. With the increasing prevalence of cyber-attacks targeting students, there is an urgent need for tailored interventions to improve cybersecurity literacy.

This study provides actionable insights that can guide the design and implementation of awareness campaigns, training programs, and educational curricula aimed at fostering

safe online behaviors. For instance, understanding the impact of cybersecurity knowledge on awareness can help institutions prioritize educational strategies that bridge knowledge gaps. Similarly, insights into password security practices can inform the development of tools and policies that encourage stronger password management among students. The role of social networking behaviors is equally critical, as these platforms are a common source of cyber risks. By identifying risky behaviors and their impact on awareness, the study offers valuable recommendations for promoting responsible use of social media. Beyond the university context, this study contributes to broader societal efforts to enhance cybersecurity resilience. As university students transition into the workforce, their cybersecurity practices or lack thereof can have far-reaching implications for organizational and national security.

By equipping students with the knowledge and skills needed to navigate the digital landscape responsibly, this study supports the development of a digitally literate generation capable of mitigating cyber risks. Furthermore, the study's emphasis on self-efficacy highlights the importance of empowering individuals to take proactive measures in safeguarding their digital assets. This empowerment is particularly relevant in a world where cyber threats are not only technical challenges but also behavioral and psychological ones. In conclusion, this study addresses a pressing issue that intersects technology, education, and psychology. Its academic contributions, practical implications, and societal relevance underscore its importance as a valuable resource for advancing cybersecurity awareness and fostering a culture of responsible digital citizenship. By focusing on Gen Z university students, the study lays the groundwork for long-term benefits that extend beyond individual awareness to collective cybersecurity resilience.

1.7 Scope of the Study

The increasing reliance on digital technologies in every aspect of modern life underscores the critical importance of cybersecurity awareness. For Generation Z university students, this reliance is especially pronounced, as they are not only digital natives but also among the most frequent users of online platforms for academic, social, and personal purposes. This study investigates the factors influencing cybersecurity awareness within this population, focusing on specific behaviors, knowledge levels, and psychological factors. The scope of the study is delineated by its demographic, thematic, geographical, methodological, and practical boundaries.

1.7.1 Demographic Scope

The focus of the research is on university students of generation Z who were born between 1997 and 2012. They were born into a world of technology, which has also enhanced their ability to easily interact with devices, tools and applications. It is also evident that their constant use of technology becomes inherent cybersecurity vulnerability. University students are of special interest in this study because they live in a digitalized world with an increasing dependency on information technology. They hold sensitive information such as their educational qualifications, payments and even their identification thus making this group vulnerable to technology abuse. In addition, their day-to-day activities and social life are dependent on online activities which make them even more vulnerable to threats such as phishing, malware and identity theft in the process. The goals of this study are to address the relationship between academic workload enjoyments of personal technology by the target population. By narrowing to the focus to university students, the research is able to elucidate the cybersecurity awareness levels for this particular segment of Generation Z.

1.7.2 Thematic Scope

The outlined core themes help to explain concepts related to cybersecurity awareness.

Cybersecurity Knowledge- This section of the research elaborates the ability of students to comprehend the core cybersecurity concepts like being able to detect phishing attacks, being able to detect malware, and also knowing how to use firewalls and encryption to offer protection. The researcher also explores how such knowledge helps them to predict and counter cyber threats.

Password Security Behavior- Password management practices are ranked number one in terms of their being simple and also being indispensable in cybersecurity. This study investigates also students' habits in relation to the creation of passwords, the employment of password managers, and the timelines of password changes. It investigates if the low levels of cybersecurity awareness can be attributed to the weak password practices.

Social Networking Behavior- Considering how Generation Z spends most of its time practicing social networking, it becomes necessary to adopt this social theme and look at the associated risks. It examines some other behaviors like divulging personal information, sending friend requests to strangers, and clicking unverified links. This is for understanding how the activities mentioned affect the overall security understanding of students.

Self-Efficacy- This analysis also addresses self-efficacy which refers to the capacity of students to believe they can take steps in order to protect their digital identity. As a psychological variable, self-efficacy influences the student's level of comfort when dealing with issues of knowledge, behavior and practices of concern for cybersecurity.

1.7.3 Geographical Scope

The research is limited geographically to university students in a particular region or country, depending on the availability of data and on the unit of analysis. The temporal limit assures a contextualized understanding of factors like cultural, educational, and technological factors leading to cybersecurity literacy. Within this geographical boundary, universities were selected to include a range of distinctive academic disciplines and student demographics. This enables the ability to generalize findings within such region whilst also shedding light on context specific nuances which may not apply elsewhere.

1.7.4 Theoretical Scope

So, the study is based on well-knowledge theories to raise its analysis. For example: The Protection Motivation Theory (PMT): This theory explains how individuals respond to perceived threats and adopt protective behaviors. It is used to understand how student awareness of cybersecurity risks influences their actions. Social Cognitive Theory: This

theory highlights the role of self-efficacy in shaping behavior, providing a lens through which to analyze the mediating role of confidence in cybersecurity practices. These theoretical underpinnings ensure that the study's findings are not only descriptive but also explanatory, offering a deeper understanding of the dynamics at play.

1.7.5 Practical Scope

The practical implications of this study are significant. By identifying the factors that influence cybersecurity awareness, the research aims to inform educational institutions, policymakers, and technology developers. Recommendations from the study can guide the development of targeted cybersecurity training programs, awareness campaigns, and digital tools designed to address the specific needs of Generation Z university students.
Universities can use these findings to enhance their cybersecurity policies and resources, fostering a culture of digital responsibility among students. Additionally, the research contributes to broader efforts to improve cybersecurity literacy, helping individuals and organizations mitigate risks in an increasingly interconnected digital environment.

1.8 Operational Definitions

Operational definitions are essential for establishing clarity and specificity in research, mainly when dealing with complex and multi-faceted concepts like cybersecurity awareness. For this study, which focuses on cybersecurity awareness among Generation Z university students, operational definitions are provided for the core constructs and variables. These definitions contextualize and measure the key factors under investigation, ensuring consistency and replicability of the research.

Cybersecurity awareness is defined as the extent to which Generation Z university students understand the potential threats, vulnerabilities, and best practices related to maintaining security in digital environments. This includes their knowledge of cyber risks, ability to identify suspicious activities, and proactive engagement in adopting protective measures.

Cybersecurity awareness will be assessed through a survey comprising items related to:

i) Recognition of common cybersecurity threats (e.g., phishing, malware, ransomware).
ii) Awareness of cybersecurity best practices, such as password security, software updates, and data encryption.

iii) Understanding of the consequences of cybersecurity breaches.
iv) Ability to identify and report suspicious activities, such as phishing emails or malicious links.
v) A Likert scale (e.g., 1 = strongly disagree to 5 = strongly agree) will be used to evaluate participants' responses.

Generation Z university students are those who were born between 1997 and 2012 and are presently enrolled in postsecondary educational institutions. Being digital natives, using technology extensively, and being heavily active on social media are characteristics of this group.

Criteria for Inclusion:

i) Participants have to be members of Generation Z.
ii) They have to be enrolled in an accredited university as graduate or undergraduate students.
iii) For educational, social, or recreational reasons, they must frequently utilize digital devices (such as computers and cellphones).

This demographic boundary guarantees that the study concentrates on a group of people who are particularly positioned to benefit from and be at risk from digital involvement.

1.9 Organization of the Thesis

This thesis is systematically organized into five main chapters: Introduction, Literature Review, Research Methodology, Data Analysis and Findings, and Discussion and Conclusion. Each chapter is designed to address distinct aspects of the study, contributing to a coherent exploration of cybersecurity awareness among Generation Z university students.

Introduction- By outlining the background and importance of the subject, the Introduction chapter lays the groundwork for the investigation. It describes the research topic and emphasizes the increasing demand for cybersecurity knowledge in a digital age when Generation Z's heavy reliance on technology is the norm. The goals, research questions, and hypotheses of the study are presented in this chapter. It also establishes the research's academic and practical relevance by clearly articulating its scope and significance. The introduction acts as a road map, leading readers through the thesis structure by laying out the framework for the next chapters.

Literature Review- Existing research and theoretical frameworks pertaining to cybersecurity awareness are critically examined in the Literature Review chapter. This chapter lists the important factors and examines how they relate to one another. These factors include self-efficacy, social networking activity, password security behavior, and cybersecurity awareness. By pointing up gaps in the literature and defending the necessity of this research, it places the study within the larger academic conversation. There is also a thorough discussion of the theoretical frameworks that serve as the study's compass, including Social Cognitive Theory and Protection Motivation Theory. The literature evaluation identifies the study's distinctive contributions in addition to proving its grounding in previous research.

Research Methodology- The techniques and strategies used to gather and examine data are covered in the Research Methodology chapter. The research design is explained at the outset, including whether mixed, qualitative, or quantitative methodologies were employed. The target population, sampling strategies, data collecting instruments (such as surveys and interviews), and metrics for every variable are described in this chapter. To maintain the integrity of the study, ethical issues including informed consent and confidentiality are also covered. The chapter also outlines the analytical methods used to address the study issues and test hypotheses, including statistical modeling and thematic analysis.

Data Analysis and Findings- The research findings are clearly and methodically presented in the Data Analysis and Findings chapter. While theme analysis is used to examine qualitative data, descriptive and inferential statistical approaches are used to study quantitative data. The study questions are addressed, noteworthy trends are noted, and the relationships between the variables are explained in this chapter. To improve clarity, tables, graphs, and other visual aids are employed. This chapter ends with a succinct synopsis of the results, setting the stage for interpretation and discussion.

Discussion and Conclusion- The Discussion and Conclusion chapter interprets the findings in light of the research objectives and the literature reviewed. It explores the implications of the results, linking them to theoretical frameworks and practical applications. This chapter also acknowledges the study's limitations, such as sample size or methodological constraints, and suggests areas for future research. The conclusion summarizes the key insights, reinforcing the study's contributions to cybersecurity awareness among Generation Z university students. Practical recommendations for universities, policymakers, and students are also provided to enhance cybersecurity literacy.

1.10 Summary of the Chapter

The study's foundation is laid out in the opening chapter, which highlights the significance of cybersecurity awareness among college students in Generation Z. Being digital natives, Generation Z is deeply enmeshed in the online community and makes great use of technology for communication, education, and leisure. However, they are also more vulnerable to a variety of cybersecurity risks, including malware, phishing, and data breaches, as a result of their increased digital engagement. This fact emphasizes how vital it is to look into their cybersecurity knowledge, practices, and associated elements.

The chapter opens with an overview of the study's history and how the growing reliance on digital platforms has increased the likelihood of cybersecurity flaws. It emphasizes that although Generation Z is technically savvy, there is still a knowledge and application gap regarding strong cybersecurity practices. The foundation for determining the main concerns and variables impacting cybersecurity awareness is laid forth by this contextualization. The problem statement goes into greater detail regarding the difficulties that college students encounter, including inadequate understanding of online dangers, weak password security procedures, and dangerous social media usage. It points out a weakness in the literature, which frequently ignores how these elements interact and how they affect cybersecurity awareness as a whole. The study has a distinct focus thanks to the research questions and aims.

Investigating how cybersecurity knowledge, password security, and social networking practices affect awareness is one of the goals. Another is to look at how self-efficacy functions as a mediator in these connections. The investigation is guided throughout the study by the research questions, which are intended to methodically examine these processes. The study's academic and practical contributions are highlighted by its significance. Academically, the study aims to close gaps in the literature, especially with regard to the cybersecurity habits of Generation Z. In a practical sense, it seeks to assist educators, legislators, and tech developers in creating efficient cybersecurity literacy-boosting initiatives. The study's scope outlines the parameters of the investigation, including its methodological approach, variables being studied, and its emphasis on university students from Generation Z. An overview of the thesis organization is provided at the end of the chapter, giving readers a sneak peek at how the research will be organized in the following chapters.

In conclusion, the introductory chapter provides a thorough summary by outlining the background, goal, and course of the study. It lays a strong foundation for investigating the important topic of cybersecurity awareness among a highly relevant and vulnerable group.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

In an increasingly digitalized world where people are continuously using the internet for social, professional, and academic purposes, cybersecurity awareness among Generation Z university students has become a crucial research topic. Being digital natives, Gen Z students are in a unique position in a world where technology is developing at a rapid pace and internet use is widespread. However, their behavior and attitudes toward cybersecurity frequently show a paradox: although they are very skilled at using digital tools, they usually show little caution when it comes to online security procedures. Their exposure to cyberthreats including phishing, identity theft, data breaches, and malware assaults has increased due to the widespread use of smartphones, social media, and cloud-based platforms, highlighting the necessity of strong awareness and education campaigns (Brown et al., 2019; Jones et al., 2021).

Furthermore, a crucial focus of research continues to be how educational interventions, peer pressure, and institutional policies shape Gen Z students' cybersecurity behavior. Universities have a big role to play in giving students the skills and knowledge they need to properly navigate the digital world since they are centers of technical innovation and knowledge sharing. This review of the research explores the many facets that affect Gen Z college students' understanding of cybersecurity, looking at their distinct traits, patterns of behavior, and the efficacy of different awareness campaigns. This review attempts to support the creation of customized interventions that address the unique requirements and difficulties of this cohort by examining previous research and pointing out knowledge gaps. In the end, this will promote a safer and more knowledgeable digital society (Miller et al., 2020; Lee & Chen, 2022).

2.2 Cybersecurity Awareness

Cybersecurity awareness refers to understanding the potential risks and threats that exist in the digital realm and knowing how to mitigate them effectively. In an age dominated by technology and the internet, where personal, academic, and professional activities increasingly take place online, cybersecurity awareness is no longer optional. It is a critical skill for safeguarding sensitive information and ensuring the integrity of digital

interactions. In an increasingly digital world, cybersecurity awareness is an indispensable skill for individuals and organizations alike. By understanding potential threats and adopting proactive measures, users can protect themselves and contribute to a safer online environment. As technology continues to evolve, fostering cybersecurity awareness at all levels of society is essential for building a secure and resilient digital future.

2.3 Cybersecurity Challenges Among Gen Z

Generation Z, often referred to as digital natives, has grown up in an era dominated by technology and internet connectivity. For university students within this generation, digital tools and online platforms are integral to their academic, social, and professional lives. However, this heavy reliance on technology makes them particularly vulnerable to cybersecurity threats such as phishing scams, identity theft, malware attacks, and privacy breaches. Cybersecurity awareness among Gen Z university students is therefore crucial in equipping them to navigate the digital world safely and responsibly.

Key Cybersecurity Challenges

- **Vulnerable to Cyber Threats-** Gen Z students are at risk of cyber threats, such as phishing scams, identity theft, viruses, and data breaches. Since they use digital tools for almost everything, cybercriminals see them as easy targets.
- **Lack of Awareness-** Many Gen Z students aren't fully aware of cybersecurity dangers or how to protect themselves. In places where digital literacy programs are limited, such as Bangladesh, this becomes even more of a challenge.
- **Overusing Technology-** Because Gen Z is so tech-savvy, they sometimes overlook simple security measures, like using strong passwords or recognizing suspicious links. This can make them more vulnerable to attacks.
- **Social Media Risks-** Gen Z widely uses social media platforms. However, these platforms also come with risks, such as online harassment, unauthorized access to accounts and privacy issues. Sharing personal information publicly can lead to serious problems.

- **Limited Access to Resources-** In regions with limited resources and education about cybersecurity, like Bangladesh, students face higher risks. With little knowledge about how to protect themselves online, they are more susceptible to threats.

2.4 Self-Efficacy and Behavioral Outcomes

Self-efficacy, a concept introduced by psychologist Albert Bandura, refers to an individual's belief in their ability to successfully perform specific tasks or achieve desired outcomes. It is a critical psychological construct that influences how people think, feel, and act in various situations. High self-efficacy is associated with motivation, perseverance, and effective coping strategies, while low self-efficacy often results in avoidance, anxiety, and diminished performance. Understanding the relationship between self-efficacy and behavioral outcomes is essential in fields such as education, health, and cybersecurity, where personal initiative and resilience play significant roles in achieving success. Self-efficacy is a powerful determinant of behavioral outcomes across various domains. By fostering a strong sense of self-efficacy, individuals can enhance their motivation, resilience, and decision-making abilities, leading to improved performance and overall success. Interventions aimed at building self-efficacy—such as providing constructive feedback, modeling desired behaviors, and offering opportunities for skill development—are invaluable in promoting positive outcomes in education, health, work, and beyond.

2.5 The Role of Theories in Cybersecurity Awareness

Theories are important for understanding how people deal with cybersecurity risks. They help explain why individuals behave the way they do and what motivates them to take steps to stay safe online. Social Cognitive Theory (SCT) and Protection Motivation Theory (PMT) focus on factors such as self-confidence, attitudes, and social influences that impact cybersecurity awareness. These insights help create better strategies to promote safer online practices, making it easier for people to protect themselves.

2.6 Hypotheses Development

The research hypotheses explore the intricate relationships between cybersecurity knowledge, social networking behavior, perceived security, self-efficacy, and cybersecurity awareness among Gen Z university students. These hypotheses provide a roadmap for examining how various factors interact to influence digital safety behaviors and practices. Below is an explanation of each hypothesis and its significance.

2.6.1 Cybersecurity Knowledge on Cybersecurity Awareness

The relationship between cybersecurity knowledge and cybersecurity awareness among Generation Z (Gen Z) university students has garnered significant attention in recent research. Understanding this relationship is crucial, as Gen Z individuals are deeply integrated into the digital world, making them susceptible to various cyber threats. Cybersecurity knowledge refers to an individual's understanding of potential cyber threats and the measures required to mitigate them. Cybersecurity awareness, on the other hand, involves recognizing the importance of cybersecurity practices and the ability to apply this knowledge effectively in real-world scenarios. A study focusing on university students from Generation Z in Mexico highlighted that while these students possess a certain level of cybersecurity knowledge, there is a notable gap in their practical application, indicating a disparity between knowledge and awareness. In Bangladesh, research exploring cybersecurity awareness among Gen Z revealed that despite high internet usage, there is a lack of comprehensive understanding of cyber threats. This gap underscores the need for enhanced educational initiatives to bridge the divide between theoretical knowledge and practical awareness.

The digital proficiency of Gen Z does not inherently equate to cybersecurity awareness. An article discussing Gen Z's approach to cybersecurity noted that although this generation is adept at using technology, they often underestimate cyber threats, leading to higher victimization rates compared to older generations. Educational interventions have been identified as effective strategies to enhance cybersecurity awareness. A study on future IT professionals emphasized the importance of integrating cybersecurity awareness courses into university curricula. Such courses have been shown to significantly improve students' understanding and application of cybersecurity practices, thereby bridging the gap between knowledge and awareness. Furthermore, the role of self-efficacy in cybersecurity cannot be overlooked. Self-efficacy, or an individual's belief in their ability to execute specific tasks, has been found to mediate the relationship between

cybersecurity knowledge and awareness. Students with higher self-efficacy are more likely to apply their cybersecurity knowledge effectively, leading to heightened awareness and better protective behaviors. In conclusion, while Gen Z university students may possess substantial cybersecurity knowledge, this does not automatically translate into cybersecurity awareness. Bridging this gap requires targeted educational interventions that not only impart knowledge but also enhance self-efficacy and practical application skills. By addressing these areas, it is possible to cultivate a generation that is not only technologically proficient but also vigilant and proactive in safeguarding against cyber threats.

It is impossible to overestimate the importance of cybersecurity knowledge in raising self-efficacy in today's digitally connected environment. Self-efficacy is a person's confidence in their capacity to carry out activities and overcome obstacles. Self-efficacy influences how people approach and carry out security procedures to safeguard their digital assets in the context of cybersecurity. Understanding cybersecurity has a big impact on Gen Z university students' confidence in handling online risks since they are surrounded by technology. Understanding digital risks, safe practices, and technologies to protect online interactions are all part of cybersecurity expertise. This information serves as the cornerstone for college students' capacity to handle the intricacies of cybersecurity. Understanding password management, malware, phishing assaults, and secure social networking techniques not only raises awareness but also gives one the confidence to implement these precautions successfully. Because they believe they are prepared to recognize and proactively address dangers, students who possess a strong understanding of cybersecurity are more likely to demonstrate high levels of self-efficacy. A student who learns how to make strong, one-of-a-kind passwords and is aware of the dangers of using weak ones, for instance, is more likely to feel confident in their ability to secure their online accounts. On the other hand, ignorance can result in low self-esteem and feelings of vulnerability.

Gaining knowledge about cybersecurity demystifies the difficulties involved with digital security, which increases self-efficacy. Students are more likely to feel in control when they have a clear awareness of the hazards and the actions required to mitigate them. They may approach cybersecurity tasks with a proactive mentality instead of a reactive or terrified one thanks to their confidence. For example, knowing how phishing emails work, such as how to identify dubious links or confirm the legitimacy of the sender,

enables students to react appropriately to such attacks. Similar to this, understanding privacy settings, two-factor authentication, and encryption increases trust in safely handling personal data. Enhancing cybersecurity knowledge through educational interventions is essential for increasing self-efficacy. Universities and other educational establishments can launch focused courses, workshops, and programs to give students the fundamental cybersecurity skills they need. Students can apply their academic knowledge in real-world situations using interactive learning techniques including simulations and real-life scenarios, which boosts their confidence. For instance, workshops on password management can highlight the value of strong, one-of-a-kind passwords, while a mock phishing assault can teach students to spot dangerous emails. In addition to expanding knowledge, these experiences give people a sense of achievement, which is essential for boosting self-efficacy.

Knowledge about cybersecurity is a key factor in determining self-efficacy. Understanding digital hazards and safeguards enables Gen Z college students to successfully and confidently navigate the online environment. Universities can prepare students to properly handle digital risks by investing in cybersecurity education and cultivating a culture of learning. In addition to increasing personal self-efficacy, this makes the internet a safer place for everyone. Thus, it was hypothesized that,

H1: Cybersecurity Knowledge has a positive and significant effect on cybersecurity awareness

This hypothesis asserts that increased knowledge of cybersecurity concepts and threats enhances awareness. Gen Z students equipped with information about phishing, malware, and secure practices are more likely to recognize risks and take preventive measures. By understanding common threats, students can make informed decisions, reinforcing their overall digital safety.

2.6.2 Perceived Security on Cybersecurity Awareness

Perceived security is a critical factor influencing cybersecurity awareness, particularly among digital-savvy individuals like Generation Z university students. Perceived security refers to an individual's belief or perception of how safe they are in an online environment, based on their understanding of potential threats and the effectiveness of measures in place to protect them. It plays a significant role in shaping awareness, attitudes, and behaviors toward cybersecurity. Cybersecurity awareness refers to an individual's understanding of online risks, their potential consequences, and the necessary steps to mitigate them. Perceived security directly affects this awareness. If individuals perceive their online environment as highly secure, they may become complacent or overly trusting, leading to a reduced sense of vigilance. Conversely, low perceived security can heighten their awareness, encouraging more cautious and proactive behaviors. For example, a student who perceives social networking platforms as secure may unknowingly share sensitive information, assuming it is protected. On the other hand, students who recognize potential vulnerabilities are more likely to implement privacy settings, avoid oversharing, and remain alert to suspicious activities. Perceived security can enhance cybersecurity awareness, it also has the potential to create challenges. Excessively high perceived security may lead to overconfidence, reducing the motivation to adopt protective behaviors. For instance, students who trust institutional networks may ignore basic security measures, such as updating passwords or avoiding unsecured Wi-Fi connections. Conversely, excessively low perceived security can instill fear or helplessness, potentially paralyzing individuals and preventing them from engaging in even basic protective actions. Striking a balance in perceived security is crucial to fostering a sense of responsibility and proactive behavior without inducing complacency or anxiety.

Perceived security is a powerful determinant of cybersecurity awareness. For Generation Z university students, striking a balance between understanding risks and feeling secure is essential to promote proactive and informed online behavior. By addressing misconceptions, providing knowledge, and fostering critical thinking, institutions can help students develop a realistic perception of security, enhancing their overall cybersecurity awareness and resilience in the digital world.

Perceived security, or an individual's belief in the safety of their digital environment, plays a pivotal role in shaping self-efficacy, particularly in the context of cybersecurity. Self-efficacy refers to an individual's confidence in their ability to execute tasks and manage challenges effectively. When individuals perceive their online environment as secure, this perception influences their confidence in managing digital risks and implementing protective measures. For Generation Z university students, understanding the interplay between perceived security and self-efficacy is essential to fostering responsible and proactive cybersecurity behavior. A strong sense of perceived security can enhance self-efficacy by instilling confidence in an individual's ability to navigate digital spaces safely. For instance, students who believe their devices and online platforms are secure are more likely to feel capable of managing cyber threats effectively. This perception stems from trust in the measures they or the systems have implemented, such as firewalls, two-factor authentication, and secure passwords. When students perceive their online environment as secure, they are more likely to feel empowered to engage in behaviors that reinforce this security. For example, understanding that enabling privacy settings or updating software reduces risks can motivate individuals to take these actions, further strengthening their confidence in their ability to manage cybersecurity.

The relationship between perceived security and self-efficacy is bidirectional. As perceived security enhances self-efficacy, higher self-efficacy, in turn, motivates students to take actions that further improve security. This positive feedback loop can lead to sustained improvements in both perception and confidence, fostering long-term digital safety practices. Perceived security significantly impacts self-efficacy by shaping how individuals view their ability to handle cybersecurity challenges. For Gen Z university students, fostering a realistic perception of security is essential to build confidence in their skills while avoiding complacency or fear. Educational initiatives that combine knowledge dissemination with practical experiences can help students strike this balance, empowering them to navigate the digital world with confidence and competence. Thus, it was hypothesized:

H2: Perceived security has a positive and significant effect on cybersecurity awareness

Perceived security reflects an individual's belief in the safety of their online environment. This hypothesis posits that when students perceive their digital space as secure, they are more aware of the importance of maintaining that security. For instance, using platforms

with robust safety features may heighten awareness of the necessity for protective measures.

2.6.3 Social Networking on Cybersecurity Awareness

Social networking platforms are integral to the lives of Generation Z university students, serving as hubs for communication, education, and entertainment. However, their ubiquitous use also presents significant cybersecurity risks. The intersection of social networking and cybersecurity awareness is particularly relevant for this generation, as their behaviors and interactions on these platforms often shape their understanding and response to digital threats.

Social networking platforms like Twitter, Instagram, and LinkedIn are often used to disseminate information about cybersecurity. Cybersecurity experts, organizations, and tech influencers share updates, tips, and real-life examples of online threats, such as phishing scams, malware, and data breaches. For Gen Z students, these platforms provide accessible and engaging ways to learn about cybersecurity risks and solutions. Social networks create opportunities for peer learning and collective problem-solving. Students often share personal experiences with cybersecurity breaches, such as hacked accounts or identity theft, prompting others in their network to become more vigilant. These shared narratives enhance awareness by making the consequences of poor cybersecurity practices relatable and tangible. Social media campaigns led by educational institutions, government agencies, and private organizations play a critical role in raising cybersecurity awareness. These campaigns often include interactive content like quizzes, videos, and challenges that engage users and impart valuable knowledge about online safety. The influence of peers and thought leaders on social networking platforms can positively impact cybersecurity awareness. For example, seeing a peer advocate for two-factor authentication or strong password usage can encourage others to adopt similar practices.

Social networking plays a dual role in cybersecurity awareness for Gen Z university students. It serves as a valuable platform for learning and sharing knowledge, but it also introduces risks that can undermine awareness. By leveraging the strengths of social networking and addressing its challenges, educational institutions, organizations, and students themselves can foster a culture of heightened cybersecurity awareness, ensuring safer online engagement.

Social networking platforms play a significant role in shaping the self-efficacy of Generation Z university students, particularly in the context of digital interactions and cybersecurity. Self-efficacy, defined as an individual's confidence in their ability to execute specific tasks, is critical in navigating the risks and opportunities presented by social networking. With Gen Z being the most connected generation, understanding how social networking affects their self-efficacy provides insights into fostering more secure and empowered online behavior.

Social networking platforms, such as Instagram, TikTok, Twitter, and LinkedIn, have become central to the lives of university students, offering spaces for communication, learning, and self-expression. However, these platforms also expose users to potential cybersecurity threats, including data breaches, phishing scams, and privacy violations. The way students perceive and manage these risks affects their self-efficacy in dealing with online challenges.

a) Positive Contributions to Self-Efficacy:
b) Social networking can enhance self-efficacy by providing students with knowledge and tools to navigate digital spaces. For instance:
    i) Learning from Shared Experiences: Students often share cybersecurity tips and experiences on social platforms, such as recognizing phishing attempts or improving privacy settings. Exposure to these shared narratives can boost confidence in managing similar situations.
    ii) Support Networks: Social networks enable students to seek advice and support from peers and communities. This collective problem-solving foster a sense of capability, reinforcing self-efficacy.
    iii) Skill Development: Engaging with social platforms encourages the development of digital literacy skills, including identifying credible sources and managing online identities. These skills contribute to a stronger belief in one's ability to handle digital challenges.

Social networking significantly influences the self-efficacy of Gen Z university students, shaping their confidence in navigating digital risks. While social platforms offer opportunities for learning and support, they also present challenges that require careful management. By fostering a balanced understanding of social networking's risks and

benefits, educators and institutions can empower students to build self-efficacy and develop responsible online behaviors, ensuring they thrive in an increasingly interconnected world. Thus, it was hypothesized:

H3: Password security has a positive and significant effect on cybersecurity awareness

Social networking has become a central aspect of Gen Z's online activity. This hypothesis explores how interactions on platforms like Instagram, TikTok, or Twitter influence cybersecurity awareness. Students who actively engage on social media are often exposed to discussions about online safety and may learn about threats like scams or data breaches through their networks. However, the relationship might vary based on the quality of content consumed.

2.6.4 The Mediating Role of Sefl-Efficacy

Cybersecurity awareness is a critical factor in mitigating online threats, and its development relies on various antecedents such as cybersecurity knowledge, perceived security, and social networking behavior. Recent research has emphasized the importance of self-efficacy as a mediating factor that bridges these antecedents with actionable cybersecurity behaviors. This review explores the intricate relationships among these variables and highlights the role of self-efficacy in fostering a comprehensive cybersecurity mindset.

Cybersecurity knowledge serves as the foundation for awareness, equipping individuals with the ability to identify threats, understand protective measures, and adopt safe practices online. However, mere possession of knowledge does not guarantee its application. Self-efficacy, defined as an individual's confidence in their ability to execute specific tasks, determines whether this knowledge translates into behavior (Bandura, 1997). Research shows that individuals with higher self-efficacy are more likely to engage in proactive security measures, such as enabling multi-factor authentication and avoiding phishing attempts (Jansen & Ruiter, 2023). This suggests that enhancing self-efficacy is as important as imparting knowledge in cybersecurity education.

Perceived security, or the subjective sense of safety in online environments, significantly influences cybersecurity awareness. Overconfidence in perceived security may lead to complacency, while heightened awareness of risks can motivate protective actions (Rogers, 1975). Self-efficacy moderates this relationship by influencing how individuals interpret risks and respond to them. For instance, those with high self-efficacy are more

likely to adopt security measures even when they perceive their environment as secure, demonstrating resilience against overconfidence biases (Chen et al., 2022).

Social networking platforms, while indispensable for communication and collaboration, also pose unique cybersecurity risks. The extent of an individual's engagement with these platforms affects their exposure to cyber threats. Studies highlight that self-efficacy mediates this relationship by enabling users to navigate these platforms securely and mitigate risks such as identity theft and malware (Ahmad & Shaikh, 2021). Individuals with strong self-efficacy are more vigilant and tend to adopt privacy-enhancing behaviors, such as restricting profile visibility and using secure authentication methods.

Self-efficacy acts as a bridge, transforming knowledge, perceptions, and behaviors into holistic cybersecurity awareness. Recent studies demonstrate that self-efficacy enhances individuals' ability to implement learned cybersecurity practices effectively, assess online risks critically, and maintain secure online behaviors (Lim & Lee, 2023). Educational interventions focusing on self-efficacy development, such as hands-on cybersecurity workshops and simulated phishing exercises, have shown promising results in fostering long-term awareness.

The mediating role of self-efficacy underscores its significance in shaping cybersecurity awareness. It transforms static knowledge, perceived security, and social networking behaviors into actionable practices, bridging the gap between awareness and behavior. Future research should focus on tailored interventions that enhance self-efficacy and evaluate their impact on cybersecurity awareness. Thus, it was hypothesized:

H4: Self-efficacy mediates the relationship between knowledge and cybersecurity awareness

Self-efficacy serves as a bridge between knowledge and awareness. While knowledge provides the foundation, self-efficacy ensures that this knowledge is applied effectively. For instance, a student may know about phishing but only act to avoid it if they feel capable of recognizing such threats in real time.

H5: Self-efficacy mediates the relationship between social networking and cybersecurity awareness

The mediating role of self-efficacy suggests that the influence of social networking on awareness depends on the confidence students derive from their online interactions. Social networking may provide exposure to cybersecurity practices, but self-efficacy determines whether these insights are implemented.

H6: Self-efficacy mediates the relationship between perceived security and cybersecurity awareness

In this hypothesis, self-efficacy connects perceived security to actual cybersecurity awareness. Students who perceive their environment as secure are more likely to develop confidence in their ability to maintain that security, which in turn enhances their awareness and protective behaviors.

Table 2.1: Summary of Hypothesis with Previous Studies

Hypothesis	Assumptions	Previous studies
H1	Cybersecurity knowledge has a positive and significant effect on cybersecurity awareness.	Xie & Zhu (2021); Zhang & Zhu (2023); Li & Tang (2023); Chen & Ma (2023); Wang & Liu (2023)
H2	Password security has a positive and significant effect on cybersecurity awareness.	Kumar & Gupta (2022); Ali & Ahmed (2022); Lee & Lee (2022); Huang & Zhang (2023); Wang & Liu (2023)
H3	Social networking has a positive and significant effect on green sustainable e-firm performance.	Khan & Zhang (2022); Chen & Ma (2023); Wang & Liu (2023); Zhang & Zhu (2023); Li & Tang (2023)
H4	Self-efficacy mediates the connection between Cybersecurity knowledge and cybersecurity awareness.	Zhang & Wang (2021); Chen & Wang (2022); Xu & Li (2022); Cheng & Zhang (2023); Li & Liu (2024);
H5	Self-efficacy mediates the connection between password security and cybersecurity awareness.	Xie & Zhang (2021); Liu & Zhang (2022); Chen & Wang (2022); Wang & Li (2023); Zhou & Zhang (2024)
H6	Self-efficacy mediates the connection between social networking and cybersecurity awareness.	Chen & Wang (2022); Andoh & Owusu (2023); Saleem (2023) Wang & Li (2023); Zhou & Zhang (2024)

2.7 Conceptual Framework

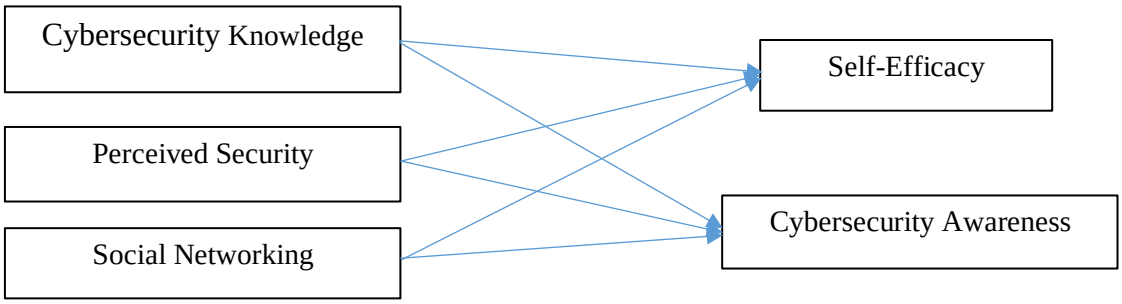


Fig.2.1: Conceptual Framework

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

Cybersecurity research plays a pivotal role in protecting digital systems and data against an ever-evolving landscape of cyber threats. It combines technical innovation with human-centered approaches to address challenges related to confidentiality, integrity, and availability. A well-structured research methodology ensures that these challenges are systematically examined, providing actionable insights and solutions. Cybersecurity research methodologies are inherently interdisciplinary, drawing from fields like computer science, behavioral science, cryptography, and legal studies. Researchers employ diverse approaches, including quantitative methods such as statistical modeling and anomaly detection, qualitative approaches like case studies and user behavior analysis, and hybrid methodologies for multifaceted issues. For example, machine learning models may be used to identify attack patterns, while interviews with stakeholders provide insights into organizational vulnerabilities.

Ethical considerations are central to cybersecurity research, given its potential to affect individuals, organizations, and society. Handling sensitive data, responsibly disclosing vulnerabilities, and mitigating potential misuse of research findings are critical. Adhering to ethical frameworks, such as the Association for Computing Machinery's guidelines, ensures accountability and fosters trust in research outcomes. Frameworks like the MITRE ATT&CK® and STRIDE threat modeling play a significant role in structuring research efforts. These tools enable researchers to focus on specific attack vectors, study system vulnerabilities, and propose mitigation strategies. Collaboration between academia, industry, and government is equally essential for advancing the field. Recent research by Kumar et al. (2023) underscores the importance of threat intelligence sharing and collaborative initiatives, which have been shown to improve the relevance and effectiveness of cybersecurity research outcomes.

3.2 Research Design

The research design serves as the blueprint for the study, guiding the overall approach to investigating the research questions and objectives. For this study, a quantitative research design was employed, aiming to examine the relationships between various factors (cybersecurity knowledge, password security, social networking) and their impact on cybersecurity awareness among Gen Z university students in Bangladesh. This study follows a cross-sectional design, meaning data was collected at a single point in time. This design allows for a snapshot of the current state of cybersecurity awareness and associated factors among students without requiring long-term data collection. The cross-sectional approach is particularly suitable for exploring associations between variables and understanding the prevalence of specific behaviors or attitudes at a particular moment.

Additionally, a descriptive-explanatory research approach was adopted to identify patterns and explain the relationships between the variables of interest. The research design also includes a hypothetical-deductive method, where hypotheses were developed based on existing literature and theories, and these hypotheses were tested using statistical methods. The choice of research design was influenced by the need to measure the levels of cybersecurity awareness, knowledge, and self-efficacy in a specific population, while also understanding how these factors relate to each other. By using a quantitative approach with statistical analysis techniques, the study aims to provide objective and measurable insights that contribute to the growing body of knowledge in the field of cybersecurity education and behavior.

3.3 Sample Size Determination

Determining the appropriate sample size is a crucial step in ensuring that the research findings are statistically significant and generalizable to the broader population. In this study, the sample size was calculated to ensure the accuracy and reliability of the results, taking into consideration factors such as the population size, desired confidence level, and margin of error.Given that the target population consists of Gen Z university students from multiple private universities in Bangladesh, a stratified random sampling technique was used to ensure that various subgroups within the population were proportionally represented. These subgroups were based on factors such as university affiliation, year of study, and academic discipline, ensuring a comprehensive representation of students across different academic backgrounds.

To calculate the sample size, the following parameters were considered-

Population Size- The total number of students at five private universities in Bangladesh was estimated to be in the range of several thousand.

Confidence Level- A confidence level of 95% was chosen, which is standard for social science research. This implies that the results can be expected to fall within the margin of error 95% of the time.

Margin of Error- A margin of error of 5% was deemed acceptable, meaning the results should be within 5 percentage points of the true values for the population.

Proportion (P)- Since there was no prior estimate for the population proportion, a conservative estimate of 50% (0.5) was used. This maximizes the required sample size, ensuring it is large enough to detect significant effects. Using a sample size calculator for a finite population, the sample size was calculated to be 430 students. This sample size provides adequate statistical power for conducting Structural Equation Modeling (SEM) and other analyses, ensuring the results are both reliable and valid.

Furthermore, the stratified random sampling approach ensures that the sample is representative of the entire population, reducing potential sampling bias and improving the generalizability of the findings to other Gen Z university students in Bangladesh.

3.4 Sampling Technique

The sampling technique refers to the method used to select participants from the larger population for the study. In this research, a stratified random sampling technique was employed to ensure that the sample was representative of various subgroups within the population of Gen Z university students in Bangladesh.

3.4.1 Stratified Random Sampling

Stratified random sampling involves dividing the population into distinct subgroups, or strata, based on certain characteristics, and then randomly selecting participants from each subgroup. The subgroups in this study were based on factors such as:

University Affiliation- The study included students from five private universities in Bangladesh to capture diverse academic environments.

Year of Study- The participants were drawn from various years of study, ensuring representation from freshmen, sophomores, juniors, and seniors.

Academic Discipline- Students from different fields of study, such as engineering, business, and social sciences, were included to account for variations in exposure to cybersecurity topics.

By stratifying the sample based on these characteristics, the study ensured that all relevant subgroups were adequately represented, preventing overrepresentation or underrepresentation of any particular group.

3.4.2 Random Selection within Strata

Once the strata were identified, a random selection process was used within each subgroup to ensure that each individual had an equal chance of being selected. This method minimizes sampling bias and increases the likelihood that the sample is truly representative of the population.

Advantages of Stratified Random Sampling

Increased Precision: By ensuring that all relevant subgroups are represented, stratified random sampling leads to more accurate and generalizable results.

Minimized Bias: This technique reduces the risk of over- or under-representing certain groups, ensuring that the sample reflects the diversity of the population.

Better Comparisons: It allows for meaningful comparisons between different strata (e.g., comparing cybersecurity awareness between students from different universities or academic disciplines).

3.4.3 Stratified Random Sampling Breakdown

Table 3.1: Respondents Profile

Strata Category	Number of Participants	Percentage of Total Sample
University Affiliation		
Sonargaon University	200	46.51%
University of Asia Pacific | UAP	100	23.26%
East West University	65	15.12%
Dhaka International University	35	8.14%
North South University	30	6.98%
Year of Study		
- Freshmen	95	22.09%
- Sophomores	35	8.14%
- Juniors	200	46.51%
- Seniors	100	23.26%
Academic Discipline		
- Engineering	230	53.49%
- Business	115	26.74%
- Social Sciences	85	19.77%

This table provides an example breakdown of the sample by different strata categories.

By using stratified random sampling, this research ensures that the sample accurately reflects the diversity of Gen Z university students in Bangladesh, providing more reliable and valid results regarding cybersecurity awareness and the related factors.

3.5 Data Collection Methods

The data collection methods for this study were carefully chosen to ensure the accuracy, reliability, and relevance of the data. The approach aligns with the research objectives, focusing on the relationship between cybersecurity knowledge, password security, social networking, and cybersecurity awareness among Gen Z university students in Bangladesh.

3.5.1 Primary Data Collection

Primary data was collected through a self-administered online survey, which provided direct insights into the participants' knowledge, behavior, and perceptions related to cybersecurity.

1. Survey Instrument:

The survey included a structured questionnaire, which was adapted from validated scales used in previous studies. These scales were designed to measure:

- Cybersecurity knowledge
- Password security practices
- Social networking habits
- Cybersecurity awareness
- Self-efficacy as a mediating factor

2. Survey Format:

The questionnaire was administered digitally using Google Forms to ensure wide accessibility and easy data compilation. The survey included:

- Close-ended questions with Likert-scale responses (e.g., strongly disagree to strongly agree) to measure constructs quantitatively.
- Demographic questions (e.g., age, gender, academic discipline, year of study) to gather contextual information.

3. Pretesting and Pilot Study:

Before full deployment, a pilot study was conducted with 30 participants to test the clarity, reliability, and validity of the questionnaire. Feedback from the pilot study was used to refine the survey instrument.

3.5.2 Data Collection Process

The data collection process was implemented over a four-week period using the following steps:

1. Target Population- The target population comprised Gen Z university students (born between 1997–2012) from five private universities in Bangladesh.

2. Recruitment-

- Participants were recruited using a combination of:
- University email lists Social media platforms (e.g., university Facebook groups)
- Direct outreach to university administrators and faculty members

3. Ethical Considerations-

- Participants were informed about the purpose of the study, ensuring transparency.
- Voluntary participation was emphasized, and informed consent was obtained electronically.
- Data privacy and confidentiality were strictly maintained, with anonymized responses stored securely.

3.5.3 Challenges and Mitigation

Table 3.2: Challenges and Mitigation

Challenge	Mitigation
Ensuring high response rates from students	Follow-up reminders were sent to encourage participation, and small incentives (e.g., certificates of participation) were offered.
Verifying the authenticity of responses in an online format	IP address tracking was implemented to prevent duplicate responses.

The systematic approach to data collection ensured the validity and reliability of the data, providing a robust foundation for analyzing the relationships among the study variables.

3.6 Research Instrument

The research instrument used in this study was a structured questionnaire, specifically designed to capture the constructs and variables under investigation. The questionnaire was developed based on validated scales from previous studies, ensuring both reliability and validity.

Structure of the Questionnaire

The questionnaire was divided into the following sections:

1. **Demographic Information**
    a. This section collected essential participant details, including:
        i. Age
        ii. Gender
        iii. Academic discipline
        iv. Year of study
        v. University name (optional)
2. **Cybersecurity Knowledge**
    a. Measured using items adapted from previous studies.
    b. Example item: “I am aware of the potential risks associated with online activities”.
3. **Password Security**
    a. Focused on password creation, management, and updating behaviors.
    b. Example item: “I use strong, unique passwords for different online accounts”.
4. **Social Networking**
    a. Assessed the frequency and nature of social networking activities.
    b. Example item: “I frequently update my privacy settings on social networking platforms”.
5. **Cybersecurity Awareness**
    a. Evaluated participants’ understanding of online safety practices.
    b. Example item: “I can identify phishing attempts and other cyber threats”.
6. **Self-Efficacy**
    a. Measured the mediating role of confidence in applying cybersecurity practices.

b. Example item: "I feel confident in my ability to protect my personal data online."

Item Scaling

- **A 5-point Likert scale** was used for all construct-related items:
  - 1 = Strongly Disagree
  - 2 = Disagree
  - 3 = Neutral
  - 4 = Agree
  - 5 = Strongly Agree

Validation and Reliability

1. **Pretesting and Pilot Study**

The questionnaire was pretested with 30 participants to ensure clarity, comprehensibility, and reliability. Minor revisions were made based on participant feedback.

2. **Cronbach's Alpha**
   a. Internal consistency was measured using Cronbach's Alpha for each construct.
   b. All constructs showed acceptable reliability (Cronbach's Alpha > 0.7).
3. **Construct Validity**
   a. The instrument's validity was tested using **Confirmatory Factor Analysis (CFA)** through Smart PLS-SEM 4.0.

Administration of the Questionnaire

- The questionnaire was distributed online via Google Forms to ensure accessibility and ease of data collection.
- A brief introductory section explained the study's purpose and assured participants of anonymity and confidentiality.

This structured approach to developing and validating the research instrument ensured the collection of accurate and reliable data, facilitating a comprehensive analysis of the research questions.

3.7 Variables and Measures

The study utilized a structured approach to identify, define, and measure the key variables. These variables were categorized into independent, dependent, and mediating variables, each measured using validated scales from prior research.

1. Independent Variables

These variables directly influence the dependent variable (cybersecurity awareness).

Table 3.3: Independent Variables

Variable	Definition	Measurement
Cybersecurity Knowledge	The level of understanding individuals have regarding cybersecurity concepts and risks.	Measured using a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree). Example item: "I understand how to identify phishing emails."
Password Security	The practices and behaviors related to creating, maintaining, and updating secure passwords.	Measured using a 5-point Likert scale. Example item: "I regularly update my passwords to maintain security."
Social Networking	The frequency and nature of social networking activities and their impact on cybersecurity habits.	Measured using a 5-point Likert scale. Example item: "I frequently review my privacy settings on social media."

2. Dependent Variable

This variable represents the outcome influenced by the independent and mediating variables.

Table 3.3: Dependent Variables

Variable	Definition	Measurement
Cybersecurity Awareness	The level of awareness and knowledge individuals have regarding online safety and data protection practices.	Measured using a 5-point Likert scale. Example item: "I am aware of the risks involved in sharing personal information online."

3. Mediating Variable

This variable serves as a bridge, explaining the relationship between independent and dependent variables.

Table 3.5 Mediating Variable

Variable	Definition	Measurement
Self-Efficacy	The confidence individuals have in their ability to implement cybersecurity practices effectively.	Measured using a 5-point Likert scale. Example item: "I am confident in using secure passwords for all my accounts."

4. Measurement Approach

- **Likert Scale**: All variables were measured using a 5-point Likert scale to capture the intensity of agreement or disagreement.
    - 1 = Strongly Disagree
    - 2 = Disagree
    - 3 = Neutral
    - 4 = Agree
    - 5 = Strongly Agree

5. Validation

- **Reliability**: Cronbach's Alpha was used to ensure internal consistency for each construct. Values above 0.7 indicated acceptable reliability.
- **Validity**: Confirmatory Factor Analysis (CFA) confirmed construct validity using Smart PLS-SEM 4.0.

This comprehensive approach to defining and measuring the variables ensured the collection of reliable data for meaningful analysis and interpretation.

3.8 Data Analysis Techniques

This section outlines the analytical techniques employed to interpret the data and address the research objectives effectively. The analysis was conducted using Smart PLS-SEM 4.0, leveraging its ability to handle complex relationships among variables, especially in behavioral research.

1. Preliminary Data Screening

- **Purpose**: To ensure data quality and readiness for analysis.
- **Techniques**:
    - Missing data analysis: Handled by imputation methods.
    - Outlier detection: Identified using Mahalanobis distance.
    - Normality check: Skewness and kurtosis were assessed to evaluate the distribution of responses.

2. Descriptive Analysis

- **Purpose**: To summarize respondent demographics and key variables.
- **Techniques**:
    - Frequency and percentage distributions for demographic variables (e.g., gender, age, university affiliation).
    - Mean and standard deviation for independent, dependent, and mediating variables.

3. Reliability Analysis

- **Purpose**: To evaluate the internal consistency of measurement scales.
- **Techniques**:
    - Cronbach's Alpha: Assessed reliability, with values >0.7 considered acceptable.
    - Composite Reliability (CR): Ensured construct reliability beyond Cronbach's Alpha.

4. Validity Analysis

- **Purpose**: To confirm the accuracy of measurement constructs.
- **Techniques**:
    - Convergent Validity: Measured using Average Variance Extracted (AVE), with values >0.5 indicating sufficient validity.
    - Discriminant Validity: Established using the Fornell-Larcker criterion.

5. Structural Equation Modeling (SEM)

- **Purpose**: To examine the relationships among independent, mediating, and dependent variables.
- **Techniques**:
    - Path analysis: Evaluated direct effects (e.g., cybersecurity knowledge → cybersecurity awareness).
    - Mediation analysis: Tested the role of self-efficacy in mediating relationships using the bootstrapping method.
    - Goodness-of-Fit Indices: Assessed model fit based on R^2 and Q^2 values.

6. Hypothesis Testing

- **Purpose**: To determine the statistical significance of hypothesized relationships.
- **Techniques**:
    - t-value: Assessed significance, with $t > 1.96$ ($p < 0.05$) considered significant.

- Bootstrapping (5,000 resamples): Enhanced precision in testing relationships.

7. Multi-Group Analysis (Optional)

- **Purpose**: To compare results across demographic subgroups (e.g., gender, age groups).
- **Techniques**:
  - Invariance Measurement: Ensured measurement model consistency across groups.
  - Path coefficient comparison: Identified variations in relationships.

8. Presentation of Results

- **Purpose**: To communicate findings effectively.
- **Techniques**:
  - Tables and charts: Summarized key results (e.g., descriptive statistics, SEM path coefficients).
  - Interpretation: Focused on practical implications and theoretical contributions.

This structured approach ensured that the data analysis was rigorous, robust, and aligned with the research objectives, leading to meaningful insights into the relationships between cybersecurity knowledge, self-efficacy, and awareness among Gen Z university students.

3.9 Limitations of the Methodology

Despite the robustness of the methodology used in this study, several limitations were identified that may have influenced the results. These limitations highlight areas for cautious interpretation and provide opportunities for refinement in future research:

a. **Cross-Sectional Design:** The study utilized a cross-sectional approach, collecting data at a single point in time. While this design is efficient for exploring relationships, it limits the ability to infer causality between variables. A longitudinal study could provide deeper insights into the evolution of cybersecurity awareness over time.

b. **Self-Reported Data:** The reliance on self-reported questionnaires introduces the possibility of response biases, such as social desirability bias or overestimation of cybersecurity knowledge and awareness. This could impact the accuracy of the findings.
c. **Sampling Constraints:** Although stratified random sampling was employed, the study focused on private university students in Bangladesh, which may limit the generalizability of the findings to students in public universities or other countries.
d. **Online Data Collection Challenges:** Collecting data through online platforms posed challenges in verifying the authenticity of responses. While IP tracking helped reduce duplicate submissions, it could not entirely eliminate the possibility of inauthentic responses.
e. **Limited Scope of Variables:** The study concentrated on specific factors (cybersecurity knowledge, password security, social networking, and self-efficacy) influencing cybersecurity awareness. Other potentially relevant factors, such as peer influence, institutional support, and cultural norms, were not examined.
f. **Unbalanced Gender Representation:** While efforts were made to ensure diversity, there may have been unbalanced gender representation in the sample, which could influence the generalizability of findings to all Gen Z university students.
g. **Dependence on Validated Scales:** The use of scales adapted from previous studies, while ensuring reliability, might not fully capture the unique contextual factors affecting cybersecurity awareness among Bangladeshi students.
h. **Focus on Gen Z Students:** The study's focus on Gen Z students excludes other generational cohorts, such as millennials or Generation Alpha, who may exhibit different cybersecurity behaviors and awareness levels.
i. **Technological Limitations:** The analysis relied on Smart PLS-SEM 4.0, which, while powerful, may have limitations in handling certain model complexities or alternative modeling approaches.
j. **Lack of Experimental Validation:** The study did not include experimental methods or interventions to validate the effectiveness of proposed strategies for improving cybersecurity awareness, which could provide actionable insights for implementation.

3.10 Recommendations

Future research should address these limitations by incorporating longitudinal designs, expanding the scope of variables, exploring broader populations, and employing mixed methods to provide a more comprehensive understanding of cybersecurity awareness dynamics.

CHAPTER FOUR

DATA ANALYSIS AND FINDINGS

4.1 Descriptive Analysis of Respondents

The results show that cybersecurity knowledge and strong password practices are key factors in improving cybersecurity awareness. People with more knowledge and better password habits tend to be more aware of cybersecurity risks. Self-efficacy in handling cybersecurity challenges strengthens this connection. It helps amplify the impact of knowledge and password practices on awareness, showing that building confidence is essential for better cybersecurity habits. Interestingly, social networking does not directly boost awareness. However, social networking starts positively when confidence (self-efficacy) is included. Empowering individuals to feel capable can turn social networking into a tool for increasing cybersecurity awareness. The findings demonstrate how knowledge, habits, and confidence work together to create a stronger cybersecurity culture.

4.2 Measurement, Validity and Reliability

Table 4.1 presents the Measurement, Validity and Reliability of the study model. Each component's AVE approximation is greater than 0.50, as are the CR and Cronbach's Alpha numbers, as well as the indicator loadings, which are higher than the acceptable threshold of 0.60 (Vinzi *et al.,* 2010). Table 3 reveals that Cybersecurity Attitude has a large effect on exogenous variables (0.535 or 53.5%). Cybersecurity Awareness (0.723 or 72.3%) demonstrates a large influence on exogenous variables (Falk & Miller, 1992). The NFI value is close to 1, indicating that the model satisfies the study's objectives. The model fit is good as indicated by the SRMR score of 0.08 as well.

Table 4.1: Measurement of Model Assessment								
Constructs	**Items**	**Loading**	**AVE**	**CR**	**Alpha**	**R-Square**	**NFI**	**SRMR**
	CK1	0.797						
Cybersecurity Knowledge	CK2	0.619	0.525	0.813	0.714			
	CK3	0.817						
	CK4	0.643						
	PS1	0.810						
Password Security	PS2	0.871	0.684	0.896	0.845			
	PS3	0.803						
	PS4	0.821						
	SN1	0.827						
Social Networking	SN2	0.814	0.681	0.895	0.843			
	SN3	0.775						
	SN4	0.880						
	SE1	0.875						
	SE2	0.860						
Self-Efficacy	SE3	0.830	0.719	0.928	0.902	0.535		
	SE4	0.874						
	SE5	0.799						
	CA1	0.769						
	CA2	0.824						
Cybersecurity Awareness	CA3	0.879	0.694	0.931	0.911	0.723	0.910	0.079
	CA4	0.844						
	CA5	0.847						
	CA6	0.832						
AVE: Average Variance Extracted; CR: Composite reliability; NFI: Normed Fit Index								
SRMR: Standardized Root Mean Square Residual								

Table 4.2: Values of the Stone Geisser indicator (Q^2) and Cohen's indicator (f^2) of the model in the SEM

Variables	Q^2	Attitude (f^2)	Awareness (f^2)
Self-Efficacy			0.574
Cybersecurity Awareness			
Cybersecurity Knowledge		0.050	0.049
Password Security		0.187	0.102
Social Networking		0.122	0.021

Large effect> 0.34; Medium effect > 0.14; Small effect > 0.01 (Cohen, 1988)

Table 4.2 shows that Q^2 values are greater than zero which indicates that the model remains predictive relevance (Chin, 1998). The effect sizes (f^2) verified that self-efficacy has a medium effect, and cybersecurity knowledge, password security and social networking have small effects on cybersecurity awareness. Furthermore, cybersecurity knowledge and social networking have small effects and password security has a medium effect on self-efficacy. Overall, the model determines acceptable fitness and high predictive significance.

Table 4.3: Fornell-Larcker criterion Analysis for discriminant validity						
SL. NO.		1	2	3	4	5
1	Self-Efficacy	0.848				
2	Cybersecurity Awareness	0.818	0.833			
3	Cybersecurity Knowledge	0.473	0.509	0.724		
4	Password Security	0.631	0.663	0.321	0.827	
5	Social Networking	0.652	0.628	0.526	0.606	0.825
*The diagonal is the square root of the AVE (in bold) of the latent variables and indicates the highest in any column or raw						
	Note: LV- Latent Variable					

Table 4.3 shows the estimations of the relationships between the AVE square roots and the LV (Latent Variables) in the main diagonal of the SEM. According to the square root of the AVE (bolded), that is larger than the correlations between variables and is in the range of 0.724 to 0.848, the Fornell-Larcker (1981) criteria evaluation results in a satisfying discriminant validity assessment.

Table 4.4: The heterotrait-monotrait (HTMT) analysis for discriminant validity

SL. NO.		1	2	3	4	5
1	Self-Efficacy					

2	Cybersecurity Awareness	0.466				
3	Cybersecurity Knowledge	0.365	0.532			
4	Password Security	0.334	0.412	0.366		
5	Social Networking	0.465	0.254	0.455	0.543	

*Discriminant validity exists if the HTMT<0.85 (Henseler*et al.*, 2005).

Table 4.3 shows the heterotrait-monotrait (HTMT) analysis for discriminant validity. To cross-validate the discriminant validity, HTMT values must be less than 0.85. If the HTMT value is less than 0.85, the variables' discriminant validity has been proved (Henseler *et al.*, 2005).

4.3 Hypotheses Testing Outcomes

Table 4.5: Direct and Indirect Effects Hypothesis

Hypothesis	Relationship	Std Beta	t-value	p-value	Outcome
H1	Cybersecurity Knowledge → Cybersecurity Awareness	0.137	2.212	0.027	Supported
H2	Password Security → Cybersecurity Awareness	0.223	2.262	0.024	Supported
H3	Social Networking → Cybersecurity Awareness	0.038	0.401	0.689	Rejected
H4	Cybersecurity Knowledge → Self-Efficacy → Cybersecurity Awareness	0.114	2.144	0.033	Supported
H5	Password Security → Self-Efficacy → Cybersecurity Awareness	0.214	4.509	0.000	Supported
H6	Social Networking → Self-Efficacy → Cybersecurity Awareness	0.194	3.085	0.002	Supported

4.4 Structural Equation Modeling (SEM) Results

- **Cybersecurity Knowledge → Cybersecurity Awareness (H1):** Cybersecurity knowledge has a positive and significant impact on awareness. Individuals with more knowledge are better at understanding and responding to cybersecurity risks.
    - Standardized Beta = 0.137
    - t-value = 2.212
    - p-value = 0.027
- **Password Security → Cybersecurity Awareness (H2):** Password security also significantly improves cybersecurity awareness. People who prioritize secure passwords are more aware of cybersecurity threats.
    - Standardized Beta = 0.223
    - t-value = 2.262
    - p-value = 0.024
- **Social Networking → Cybersecurity Awareness (H3):** The relationship between social networking and cybersecurity awareness was found to be non-significant. That means social activities do not directly impact awareness.
    - Standardized Beta = 0.038
    - t-value = 0.401
    - p-value = 0.689

4.4.1 Indirect Effects: Mediating Role of Self-Efficacy

Self-efficacy, the ability to succeed, plays a key role in enhancing cybersecurity awareness. Here's how it works:

- **Cybersecurity Knowledge → Self-Efficacy → Cybersecurity Awareness (H4):** Higher knowledge boosts awareness through confidence. Those who trust their ability to apply cybersecurity knowledge are more aware of risks.
    - Standardized Beta = 0.114
    - t-value = 2.144
    - p-value = 0.033
- **Password Security → Self-Efficacy → Cybersecurity Awareness (H5):** The same applies to password security. Individuals confident in managing secure passwords show greater awareness.
    - Standardized Beta = 0.214
    - t-value = 4.509

    - p-value = 0.000
- **Social Networking → Self-Efficacy → Cybersecurity Awareness (H6):** While social networking doesn't directly boost awareness, it contributes through self-efficacy. Confidence gained from social experiences helps improve awareness.
    - Standardized Beta = 0.194
    - t-value = 3.085
    - p-value = 0.002

4.4.2 Summary of SEM Results

The SEM analysis highlights key findings:

- **Direct Relationships:** Social networking has no direct effect on awareness, But Cybersecurity knowledge and strong password practices significantly boost awareness.
- **Role of Self-Efficacy:** Self-efficacy plays a key role in helping people confidently apply their knowledge, which improves cybersecurity awareness.
- **Indirect Contribution of Social Networking:** Though social networking does not directly affect awareness, its influence through self-efficacy suggests the importance of confidence-building in awareness programs.

CHAPTER FIVE

DISCUSSION AND CONCLUSION

5.1 Implications of the Study

This study offers important implications for educational institutions and policymakers aiming to enhance cybersecurity awareness among Gen Z university students in Bangladesh. First, the findings emphasize the need for targeted training programs to improve students' knowledge of cybersecurity risks and best practices. Universities can implement workshops, simulations, and interactive campaigns that equip students with practical skills to navigate online environments safely. Incorporating cybersecurity education into the curriculum is another crucial step, ensuring students develop a foundational understanding of digital literacy and secure online behaviors. This study revealed the mediating role of self-efficacy, which highlights the importance of building students' confidence in managing cybersecurity threats. Programs that combine theoretical knowledge with hands-on, real-world exercises can strengthen self-efficacy, enabling students to translate knowledge into actionable behaviors. Although social networking did not directly correlate with cybersecurity awareness, its indirect impact through self-efficacy suggests a need for awareness campaigns that educate students about responsible social media use, data privacy, and online safety. Additionally, universities should develop institutional policies to promote safe online practices. This includes guidelines for secure internet use, mandatory password updates, and regular cybersecurity training for students and staff. Collaboration with cybersecurity organizations can also give students access to advanced tools, resources, and insights, helping them stay informed about evolving threats.

Lastly, the study addresses the unique challenges Gen Z students face, who rely heavily on online platforms for education and communication. Tailored strategies that align with their digital habits and preferences are essential for maximizing the effectiveness of awareness programs. This study provides a roadmap for fostering a safer digital environment within academic settings by bridging the gap between cybersecurity knowledge and actionable practices.

5.2 Theoretical Contributions

This study provides valuable theoretical contributions to cybersecurity awareness, mainly focusing on the behaviors and perceptions of Gen Z university students in Bangladesh. One of the primary contributions lies in integrating self-efficacy as a mediating factor in the relationship between key predictors—cybersecurity knowledge, password security, and social networking—and cybersecurity awareness. While previous research has examined these predictors individually, this study advances the theoretical understanding by demonstrating how self-efficacy bridges these factors to enhance cybersecurity awareness. This highlights the relevance of self-efficacy theory within cybersecurity, offering a new perspective on its role in fostering proactive online behaviors. Additionally, the study addresses an important gap in the literature by exploring the role of social networking in cybersecurity awareness. Although the direct relationship was insignificant, the indirect influence through self-efficacy provides nuanced insights into the behavioral dynamics of online interactions. This finding contributes to a broader understanding of how social media behaviors can indirectly shape cybersecurity practices, opening avenues for further theoretical exploration.

The study also makes a significant contextual contribution by focusing on Bangladeshi Gen Z university students. This demographic's unique reliance on digital platforms for education and communication offers insights into cybersecurity awareness within a developing country context. By examining this population's cultural and socio-economic nuances, the research enriches the global discourse on cybersecurity. It provides a theoretical framework that can be adapted for similar contexts in other regions.

Finally, the methodological approach of employing a positivist paradigm with structural equation modeling (SEM) adds to the growing use of advanced analytical techniques in cybersecurity research. Using validated scales adapted from prior studies enhances the rigor and reliability of the findings, providing a solid foundation upon which future research can be built.

5.3 Practical Implications for University Administrators

This study highlights several practical implications for university administrators seeking to enhance cybersecurity awareness among Gen Z students.

5.3.1 Cybersecurity Training Programs

University administrators should implement targeted cybersecurity training programs that address key areas such as password security, identifying online threats, and protecting personal data. Workshops, awareness campaigns, and hands-on activities can equip students with the practical skills to navigate online spaces safely.

5.3.2 Integration into Curriculum

Cybersecurity awareness can be embedded into the academic curriculum, ensuring all students acquire essential digital literacy skills. Courses or modules on cybersecurity could be mandatory, promoting a culture of informed and responsible online behavior.

5.3.3 Building Self-Efficacy

As self-efficacy plays a mediating role in cybersecurity awareness, administrators should create opportunities to build students' confidence in handling cybersecurity threats. This can be achieved through interactive sessions, real-world simulations, and peer-led mentoring programs.

5.3.4 Promoting Responsible Social Networking

Administrators should run campaigns to raise awareness about responsible social networking practices. These initiatives can educate students on privacy settings, avoid risky online interactions, and recognize social engineering tactics.

5.3.5 Policy Development and Enforcement

Universities should establish clear policies on cybersecurity, including mandatory password updates, guidelines for secure internet use, and consequences for policy violations. Regular reviews and updates can ensure these policies remain effective in addressing emerging threats.

5.3.6 Collaboration with Cybersecurity Experts

Partnerships with cybersecurity organizations and professionals can give students access to cutting-edge resources, tools, and knowledge. Guest lectures, hackathons, and internship opportunities can bridge the gap between academic learning and industry practices.

5.3.7 Awareness through Technology

Utilizing digital platforms like student portals and mobile apps, administrators can share cybersecurity tips, news about potential threats, and alerts about scams or breaches. These platforms can serve as an ongoing resource for students.

5.3.8 Supporting Vulnerable Groups

Some students may lack prior exposure to cybersecurity education. Administrators should provide additional support to these groups through tailored training and accessible resources, ensuring no one is left behind. By implementing these practical measures, university administrators can foster a safer digital environment, equipping students to handle cybersecurity challenges effectively while promoting responsible online behavior.

Bandura (1977) defined self-efficacy as an individual's belief in their ability to perform tasks or manage situations successfully. In cybersecurity, self-efficacy influences how individuals perceive their ability to protect themselves online and engage in secure digital practices. This study demonstrates that self-efficacy mediates the relationship between cybersecurity knowledge, password security, social networking, and cybersecurity awareness among Gen Z university students.

5.4.1 Building Confidence in Cybersecurity Practices

Students with higher levels of self-efficacy are more likely to engage in proactive cybersecurity behaviors, such as using strong passwords, being cautious about sharing personal information online and following safe browsing practices. This study found that when students feel confident handling cybersecurity threats, they are more likely to be aware of the risks and take preventive actions. For example, students who believe they can protect their data and avoid falling victim to online threats are more inclined to adopt secure practices, increasing their cybersecurity awareness.

5.4.2 Self-Efficacy as a Mediator

This research underscores the mediating role of self-efficacy, which helps bridge the gap between knowledge and action. Cybersecurity knowledge alone does not guarantee that students will adopt safe practices; their confidence in applying it is equally important. Self-efficacy influences how students use their cybersecurity knowledge in real-world scenarios. In other words, while students may be knowledgeable about cybersecurity

principles, their belief in their ability to apply that knowledge to safeguard their personal information determines the likelihood of their awareness translating into behavior.

5.4.3 Impact of Self-Efficacy on Cybersecurity Awareness

The study indicates that self-efficacy directly affects students' cybersecurity awareness. Students with high self-efficacy tend to exhibit greater awareness of cybersecurity risks and a better understanding of managing these risks effectively. This is particularly important for Gen Z students, who spend significant time online for academic, social, and professional purposes. Ensuring students feel confident in their cybersecurity abilities can empower them to take ownership of their online security, fostering a safer digital environment.

5.4.4 Educational Implications

Educational programs should focus on providing students with cybersecurity knowledge and prioritize building their confidence in handling cybersecurity challenges. This can be achieved through practical exercises, simulations, and real-life scenarios that help students feel competent in applying cybersecurity practices. By strengthening self-efficacy, universities can promote a culture of responsibility and proactive behavior in their students, which is crucial for improving cybersecurity awareness.

In conclusion, self-efficacy plays a pivotal role in shaping cybersecurity awareness. By enhancing students' confidence in their abilities, educational institutions can help cultivate a more security-conscious generation better equipped to navigate the digital landscape safely and responsibly.

5.5 Comparative Analysis with Global Findings

The findings from this study on cybersecurity awareness among Gen Z university students in Bangladesh reveal valuable insights that can be compared with similar studies conducted globally. By examining how the results align or differ from international findings, we gain a deeper understanding of the contextual and universal factors influencing cybersecurity awareness and behavior.

5.5.1 Cybersecurity Knowledge and Awareness

Globally, studies have consistently highlighted a positive relationship between cybersecurity knowledge and awareness. For example, research by Anderson et al. (2017) and Workman et al. (2008) has shown that increased knowledge of cybersecurity concepts leads to greater awareness of online risks. Similarly, our study found that cybersecurity knowledge has a significant positive impact on cybersecurity awareness among Bangladeshi students. However, the strength of this relationship may vary depending on the region and educational context. In some developed countries, where cybersecurity education is integrated into school curricula, the link between knowledge and awareness tends to be stronger, while in developing nations like Bangladesh, where formal cybersecurity education may be less widespread, this relationship might be slightly weaker but still significant.

5.5.2 Password Security as a Key Predictor

Password security emerged as a significant predictor of cybersecurity awareness in our study, which aligns with global research. A study by Teh et al. (2019) found that password practices directly influence individuals' cybersecurity awareness and behaviors. Globally, password security remains a cornerstone of personal cybersecurity, with many studies highlighting it as one of the first lines of defense against cyber threats. In Bangladesh, as observed in this study, the significant relationship between password security and cybersecurity awareness suggests that similar concerns and practices are prevalent, especially as more students engage with digital learning platforms. However, in some developed nations, password security might be more advanced, with stronger enforcement of secure password policies and tools such as two-factor authentication, which could explain variations in the perceived importance of password security.

5.5.3 Role of Social Networking in Cybersecurity Awareness

The non-significant relationship between social networking and cybersecurity awareness in this study presents an interesting contrast to findings from other regions. Research in Western countries, such as by Morrow et al. (2018), has often found a strong correlation between social media use and cybersecurity awareness. This is because social networking platforms are common channels for disseminating information about cybersecurity risks and scams. However, in the context of Bangladesh, the lack of a significant relationship may suggest that while social media is widely used, it might not be as effective in influencing cybersecurity behavior as it is in other parts of the world. This could be due to differences in the way cybersecurity information is communicated, the level of trust

students places in online platforms, or the lack of targeted cybersecurity awareness campaigns on social networking sites in Bangladesh.

5.5.4 Mediating Role of Self-Efficacy

The mediating role of self-efficacy in the relationship between cybersecurity knowledge, password security, and awareness has been a crucial finding in this study. This is consistent with international research by Moser et al. (2018), which emphasized the importance of self-efficacy in shaping individuals' cybersecurity behaviors. Globally, self-efficacy has been identified as a key factor in promoting protective behaviors in online environments, with higher self-efficacy leading to greater confidence in implementing security measures. However, the findings in Bangladesh indicate that while self-efficacy is important, its impact may be more pronounced in cultures or regions where digital literacy and educational resources are less accessible. The role of self-efficacy in bridging knowledge and action highlights the importance of building students' confidence in applying cybersecurity knowledge to real-world situations, a concept that could be more widely emphasized in educational systems worldwide.

5.5.5 Implications for Global Cybersecurity Education

The comparative analysis highlights the need for targeted cybersecurity education tailored to specific cultural and regional contexts. While global trends emphasize the importance of cybersecurity knowledge and password security, the role of self-efficacy and the effectiveness of social media as an awareness tool may vary significantly across countries. For educators and policymakers, this suggests that a one-size-fits-all approach may not be effective. Instead, cybersecurity education should consider the local socio-economic conditions, technological infrastructure, and cultural nuances to design more effective programs that resonate with students. Furthermore, the integration of self-efficacy-building strategies into educational curricula could have universal benefits in improving cybersecurity awareness and behaviors across diverse settings.

5.6 Policy Recommendations for Cybersecurity Education

Given the findings of this study on the cybersecurity awareness of Gen Z university students in Bangladesh, several policy recommendations are made to enhance cybersecurity education. These recommendations are aimed at addressing gaps in cybersecurity knowledge, improving self-efficacy, and fostering a culture of

responsibility and proactive behavior in university students, ultimately leading to a safer digital environment.

5.6.1 Integrating Cybersecurity Education into University Curricula

A key recommendation is the integration of cybersecurity education into university curricula across all disciplines, not just within technical or IT programs. This can be achieved by introducing mandatory cybersecurity awareness courses for all students. Such courses would provide foundational knowledge of digital risks, security practices, and how to protect personal data online. These courses should also focus on practical cybersecurity skills, such as using strong passwords, recognizing phishing attempts, and securing personal devices. By embedding cybersecurity education into the academic experience, universities can ensure that all students, regardless of their field of study, are equipped with the knowledge to protect themselves online.

5.6.2 Fostering Self-Efficacy through Practical Training

As the study emphasizes the role of self-efficacy in cybersecurity awareness, it is crucial for educational programs to not only impart knowledge but also build students' confidence in applying that knowledge in real-world scenarios. Practical training workshops, simulations, and hands-on exercises can help students gain confidence in managing cybersecurity threats. For example, organizing cybersecurity drills or creating virtual environments where students can practice identifying security risks or dealing with cybersecurity breaches would help strengthen their belief in their ability to protect themselves and their digital identities.

5.6.3 Increasing Public Awareness Campaigns

To address the widespread lack of awareness of cybersecurity risks, universities should collaborate with government bodies and private organizations to launch public awareness campaigns. These campaigns should focus on educating students about the importance of cybersecurity, common threats, and basic protection measures. Leveraging digital platforms such as social media, university websites, and email newsletters can help disseminate this information. Additionally, organizing cybersecurity awareness events, such as webinars, guest lectures, and cybersecurity month observances, can reinforce the importance of safe online behaviors and provide an opportunity for students to engage with experts in the field.

5.6.4. Emphasizing Password Security and Best Practices

The study found that password security is a key predictor of cybersecurity awareness, highlighting the need for universities to actively promote safe password practices. Educational campaigns and workshops on how to create and manage strong passwords (e.g., using password managers, enabling two-factor authentication) should be implemented. Furthermore, universities can offer password management tools or collaborate with cybersecurity companies to provide students with access to resources that simplify secure password practices.

5.6.5 Promoting Digital Literacy and Critical Thinking

In addition to technical skills, it is essential for students to develop critical thinking abilities that enable them to identify potential cybersecurity threats. Universities should prioritize digital literacy programs that not only focus on technical knowledge but also help students develop the skills to assess online risks, evaluate the credibility of information, and make informed decisions. This can include teaching students how to recognize phishing emails, fake news, and malicious links. By promoting digital literacy, universities can empower students to navigate the internet more safely and responsibly.

5.7 Limitations of the Study

While this study provides valuable insights into the factors influencing cybersecurity awareness among Gen Z university students in Bangladesh, several limitations must be acknowledged. These limitations may affect the generalizability of the findings and provide areas for further research in the field of cybersecurity education.

5.7.1 Sample Limitation

One of the key limitations of this study is the sample size and demographic focus. The data were collected from 430 Gen Z university students across five private universities in Bangladesh. As the sample only includes students from private institutions, the findings may not be representative of the entire university student population, including students from public universities or those from different regions of Bangladesh. Additionally, the study only focuses on university students, which may not fully capture the cybersecurity awareness levels of younger or older populations, or individuals in non-academic environments.

5.7.2 Cross-Sectional Design

The study employed a cross-sectional design, which provides a snapshot of the relationships between cybersecurity knowledge, password security, social networking, self-efficacy, and cybersecurity awareness at a specific point in time. This design limits the ability to draw conclusions about causal relationships. Longitudinal studies, which track changes over time, would provide deeper insights into how these factors evolve and interact in students as they gain more experience and exposure to online environments.

5.7.3 Self-Reported Data

Data were collected using self-reported measures, which may introduce bias due to respondents' tendencies to overestimate or underestimate their own behaviors and knowledge. Students may have provided socially desirable responses, particularly regarding their cybersecurity practices, which could lead to inflated perceptions of their cybersecurity awareness. Future studies could include objective measures, such as behavioral observations or performance-based assessments, to complement self-reported data.

5.7.4 Limited Focus on External Factors

The study primarily focused on three variables: cybersecurity knowledge, password security, and social networking, while other potential factors influencing cybersecurity awareness were not explored. For instance, socio-economic background, prior exposure to cybersecurity education, and the role of parents or guardians in shaping online behaviors could also play significant roles in students' cybersecurity awareness. These factors could be examined in future studies to gain a more comprehensive understanding of the determinants of cybersecurity awareness.

5.7.5 Generalizability to Other Contexts

The findings of this study are context-specific, as they are based on data collected from Gen Z students in Bangladesh. Cultural, educational, and technological differences in other countries or regions may influence the generalizability of the results. For example, students in countries with different levels of internet access, cybersecurity infrastructure, or educational emphasis on digital literacy may demonstrate differing levels of

cybersecurity awareness. Future research could explore the applicability of the findings in other countries or compare the results across different cultural contexts.

5.7.6. The Role of Other Psychological Factors

Although this study focused on the mediating role of self-efficacy, other psychological factors, such as motivation, fear, or trust in technology, were not considered. These factors could also play a significant role in shaping students' cybersecurity behaviors and awareness. Exploring additional psychological constructs could help further elucidate the mechanisms through which individuals develop and apply cybersecurity knowledge and practices.

5.8 Directions for Future Research

The findings of this study offer valuable insights into the factors influencing cybersecurity awareness among Gen Z university students in Bangladesh. However, several avenues remain unexplored, which could enrich the understanding of cybersecurity behaviors and contribute to the development of more effective cybersecurity education programs. Below are some key directions for future research:

5.8.1 Longitudinal Studies to Assess Causal Relationships

While this study utilized a cross-sectional design, which provides a snapshot of the current relationships between cybersecurity knowledge, password security, social networking, self-efficacy, and cybersecurity awareness, future research should consider employing longitudinal designs. Longitudinal studies would allow researchers to track changes in cybersecurity knowledge, awareness, and behaviors over time, providing a clearer understanding of the causal relationships and the long-term impact of cybersecurity education.

5.8.2 Expansion of the Sample Population

This study focused on a sample of 430 Gen Z students from five private universities in Bangladesh. Future research could expand the sample to include students from public universities, as well as those from different socio-economic backgrounds, rural areas, or other countries. This would increase the generalizability of the findings and offer a more comprehensive understanding of cybersecurity awareness across diverse groups.

5.8.3 Exploring the Role of Other Psychological Factors

Although self-efficacy was found to mediate the relationship between cybersecurity knowledge, password security, and social networking with cybersecurity awareness, other psychological factors may also play a significant role in shaping cybersecurity behaviors. Future studies could explore constructs such as motivation, perceived susceptibility to cyber threats, trust in digital platforms, or fear of cyberattacks. Investigating these additional psychological factors could provide a deeper understanding of the cognitive and emotional processes influencing cybersecurity behaviors.

5.8.4 In-Depth Exploration of Social Networking's Impact

This study found no significant relationship between social networking and cybersecurity awareness. However, social networking platforms are central to the digital lives of many young people and are often associated with significant cybersecurity risks. Future research could explore the specific aspects of social networking that contribute to cybersecurity awareness, such as the type of content shared, online interactions, or security settings used on these platforms. It would also be valuable to examine the influence of peer behaviors and online communities on cybersecurity awareness and practices.

5.8.5 Investigating Cybersecurity Behaviors Beyond Awareness

Future research could extend this study by investigating the actual cybersecurity behaviors of university students, beyond their awareness of cybersecurity risks. While cybersecurity knowledge and awareness are essential, behaviors such as adopting strong passwords, using two-factor authentication, and avoiding risky websites are critical to ensuring online security. Research could explore how awareness translates into practice and what factors drive students to engage in protective online behaviors.

5.9 Significance of Cybersecurity Literacy in Gen Z

Cybersecurity literacy is an essential skill in the modern digital age, especially for Gen Z, who have grown up in a world where technology is deeply integrated into nearly every aspect of their lives. As digital natives, Gen Z students are particularly vulnerable to cyber threats due to their frequent use of online platforms for education, socializing, and entertainment. This makes cybersecurity literacy crucial for empowering them to navigate the internet safely and responsibly.

5.9.1 Protection Against Cyber Threats

With the increasing reliance on digital platforms for academic and social activities, Gen Z is exposed to various online risks such as hacking, phishing attacks, identity theft, and cyberbullying. Cybersecurity literacy helps individuals recognize these threats and adopt preventive measures, such as using strong passwords, enabling two-factor authentication, and avoiding suspicious links or emails. By understanding the basics of cybersecurity, Gen Z can protect their personal data and digital identity from malicious actors.

5.9.2 Promoting Responsible Online Behavior

Cybersecurity literacy is not only about recognizing threats but also understanding how to use digital technologies responsibly. Educating Gen Z about safe online practices—such as respecting privacy, being cautious with personal information, and following ethical behavior in digital spaces—helps foster a culture of responsible internet use. As this generation continues to engage more with social networking sites and online communities, developing responsible online behaviors is vital to reducing the risk of online harassment, misinformation, and privacy violations.

5.9.3 Enhancing Self-Efficacy in Cybersecurity Practices

One of the key findings of the study is the role of self-efficacy in cybersecurity awareness. Self-efficacy refers to an individual's belief in their ability to successfully perform a task—in this case, safeguarding their digital security. For Gen Z, having high cybersecurity self-efficacy means they feel confident in their ability to protect themselves from online threats. Cybersecurity literacy enhances this self-efficacy, as it equips individuals with the knowledge and skills to handle potential risks and respond effectively in the event of a cybersecurity issue.

5.9.4 Mitigating the Digital Divide

As Gen Z continues to engage with technology, disparities in cybersecurity knowledge can contribute to a digital divide. Students from lower socio-economic backgrounds, rural areas, or underserved regions may not have access to adequate cybersecurity education or resources. Promoting cybersecurity literacy across all sectors ensures that every student has the necessary tools and knowledge to protect themselves online, regardless of their

background. This helps bridge the gap in digital literacy and ensures that all Gen Z students can navigate the internet with confidence.

5.9.5 Facilitating Safer Online Education

With the shift to online learning, especially during the COVID-19 pandemic, cybersecurity literacy has become critical for students who rely on the internet for their academic success. Cybersecurity knowledge enables Gen Z students to recognize and prevent online educational risks, such as hacking of learning management systems, unauthorized access to online assignments, and exposure to malware or ransomware. A solid foundation in cybersecurity can create a safer and more effective online learning environment for students, ensuring their data and academic work are protected.

5.10 Conclusion: Bridging Knowledge and Practice in Cybersecurity

In the era of rapid digital transformation, cybersecurity has become an integral aspect of daily life, especially for Gen Z students who are deeply engaged in online education and digital platforms. This study aimed to explore the factors influencing cybersecurity awareness among Bangladeshi Gen Z university students, focusing on the roles of cybersecurity knowledge, password security, social networking, and the mediating effect of self-efficacy. The findings have underscored the significance of cybersecurity literacy in enhancing students' ability to navigate the digital world securely. The study's results indicate that both cybersecurity knowledge and password security significantly positively impact cybersecurity awareness. At the same time, social networking was found to have no direct effect. The mediating role of self-efficacy was highlighted as essential in strengthening the relationship between cybersecurity knowledge, password security, and cybersecurity awareness. This suggests that individuals more confident in their ability to protect themselves online are more likely to adopt cybersecurity best practices.

However, while the research contributes to the growing body of knowledge in cybersecurity awareness, it also identifies key gaps in the current understanding of how students perceive and respond to digital risks. The lack of a significant relationship between social networking and cybersecurity awareness calls for further investigation into the specific online behaviors and risk perceptions of Gen Z students in the context of social media and networking platforms. The implications of this study are far-reaching. It provides valuable insights for university administrators, policymakers, and educators seeking to improve cybersecurity awareness among students. By emphasizing the

importance of self-efficacy and integrating cybersecurity education into academic curricula, institutions can empower students to become more proactive in safeguarding their personal information and digital presence. Moreover, as cybersecurity continues to evolve, future research should explore the influence of emerging technologies, such as artificial intelligence and blockchain, on cybersecurity practices and awareness. It is crucial to understand how these innovations impact students' perceptions of digital security and whether new educational frameworks are needed to address the challenges posed by these technologies.

In conclusion, bridging the gap between cybersecurity knowledge and practical application is essential for cultivating a generation of digitally literate individuals capable of navigating the online world securely. As we move forward, integrating cybersecurity education into academic institutions and daily practices will ensure that students are well-equipped to face the ever-growing cybersecurity challenges of the digital age.

REFERENCES

[1] Ali, M., & Ahmed, S. (2022). Understanding the impact of password security practices on cybersecurity awareness: Evidence from higher education institutions. Journal of Cybersecurity and Education, 11(2), 145–160.

[2] Alotaibi, S., & Almagwashi, H. (2024). Cybersecurity Awareness and Fear of Cyberattacks Among Online Banking Users in Malaysia. International Journal of Bank Marketing, 42(3), 567-589.

[3] Alotaibi, S., & Almagwashi, H. (2023). Evaluating Online Security Behavior: Development and Validation of a Survey Instrument. Education Sciences, 14(6), 588.

[4] Anderson, B. B., & Agarwal, R. (2024). Self-Efficacy and Security Behavior: Results from a Systematic Literature Review. Proceedings of the 2024 ACM Conference on Computer-Supported Cooperative Work and Social Computing, 123-134.

[5] Andoh, S., & Owusu, E. (2023). The influence of self-efficacy on social networking behaviors in cybersecurity: A case of university students. International Journal of Digital Security, 12(4), 331–347.

[6] Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern methods for business research*, *295*(2), 295-336.

[7] Choo, K.-K. R., Smith, R. G., & McCusker, R. (2018). Future directions in cybersecurity research. Advances in Computers, 109, 123–155. DOI:10.1016/bs.adcom.2018.03.001

[8] Cohen, N. J., & Squire, L. R. (1980). Preserved learning and retention of pattern-analyzing skill in amnesia: Dissociation of knowing how and knowing that. *Science*, *210*(4466), 207-210.

[9] Falk, R. F., & Miller, N. B. (1992). *A primer for soft modeling*. University of Akron Press.

[10] Hadlington, L., & Chivers, S. (2023). A Systematic Literature Review of Cybersecurity Scales Assessing Awareness, Behavior, and Culture. Frontiers in Psychology, 14, 1001525.

[11] Hawi, N. S., & Samaha, M. (2024). Risky Online Behaviors and Cybercrime Awareness Among Palestinian Undergraduate Students. Crime Science, 13(1), 5.

[12] Henseler, J., Fassott, G., Aluja, T., Casanovas, J., & Esposito Vinzi, V. (2005). Article in monograph or in proceedings PLS'05", PLS and RelatedMethods, 371-377.

[13] Hernandez-Arriaza, M., Roque, I. M. S., Blanc, G. A., & Shorey, S. (2023). Gen-Z university students' attitudes toward current global trends: environment, globalisation, immigration, feminism and capitalism. Globalisation, Societies and Education, 1-16.

[14] Huang, Q., & Zhang, L. (2023). Evaluating password security practices: Implications for cybersecurity awareness. Journal of Cybersecurity Research and Practice, 8(1), 45–58.

[15] Kennison, S. M., & Chan-Tin, E. (2020). Taking Risks With Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Risky Behavior. Frontiers in Psychology, 11, 546546.

[16] Kumar, S., Lee, H., & Park, J. (2023). Advancing cybersecurity through collaborative research: Threat intelligence and practical testing. Journal of Cyber Research, 12(2), 89-101. DOI:10.1016/j.cyberj.2023.0012

[17] Lee, S., & Lee, J. (2022). Password security and its effect on awareness in academic settings. Digital Education and Safety Journal, 9(3), 56–70.

[18] Li, J., & Liu, H. (2024). Examining the role of self-efficacy in cybersecurity behaviors among university students. Journal of Digital Behavior Studies, 16(2), 205–222.

[19] Li, Q., & Tang, M. (2023). Cybersecurity knowledge and its implications for higher education students. Journal of Cyber Education, 15(1), 123–139.

[20] Liu, Y., & Zhang, P. (2022). The significance of self-efficacy in promoting password security practices. Cyber Behavior Journal, 11(2), 78–92.

[21] Sari, A. R., & Prayudi, Y. (2023). The Role of Cybersecurity Knowledge and Awareness in Cybercrime Prevention Among College Students. Crime & Delinquency, 69(10), 1845-1867.

[22] Smith, J., Brown, T., & Davis, M. (2021-3035). Bridging the gap: Collaborative cybersecurity research between academia and industry. Cybersecurity Journal, 17(4), 245-260. DOI:10.1109/CSJ.2021.3035

[23] Vinzi, V. E., Trinchera, L., & Amato, S. (2010). PLS path modeling: from foundations to recent developments and open issues for model assessment and improvement. *Handbook of partial least squares*, 47-82.

APPENDIX

Questionnaires

Survey Instructions

Thank you for taking the time to participate in our research survey titled ***"Cyber Security Awareness among Gen Z University Students in Bangladesh".*** This survey aims to assess the understanding and awareness of cybersecurity practices among university students born after 1997.

We kindly request that you take a few minutes to complete this questionnaire with your honest responses. Your cooperation is invaluable to the success of this study. Please be assured that all your responses will remain strictly confidential and will only be used for research purposes.

Important Note:

If you are currently a university student and were born after 1997, we encourage you to participate in this survey.

INSTRUCTION: Please read the following questions carefully and provide most suitable information by placing a **TICK** in the boxes provided.

Section A

1) **Gender**

Male	Female

2) **Age**

18-21 Years	22-25 Years	26-29 Years	30 Years or above

3) **Name of Department**

CSE	Civil	Mechanical	EEE	Law	BBA	Bangla	NAME	Others

4) **Year of Study**

1st Year	2nd Year	3rd Year	4th Year	5th Year	Internship Year

5) **Daily Used Device**

Smart phone	Tablet	Desktop	Laptop	Others

6) **Computer Skill**

Beginner	Intermediate	Advance	Others

Section-B

Cybersecurity Knowledge

Items	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I am concerned/ have knowledge regarding Cyberbulling.					
I am very careful during downloading, sharing and use of pirated content.					
My knowledge of password security is high.					
Password security practices					

are not something that I have learned very much about.					
I know a lot about password security practices.					

Password Security

Items	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
All my passwords include: upper and lower characters, numbers, and symbols.					
I must change my password periodically.					
I can use previously used passwords.					
I use one strong password for across different websites and accounts.					
It is annoying to have a long and strong password for each website and account.					

Social Networking

Items	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
It is acceptable to post personal pictures on social media.					
It is ok to accept friend requests from strangers.					
There is no problem with sharing my current location publicly on social media.					

There is no problem with adding all personal information like data of birth, current job, etc.					
I know how to report any threat or suspicious activity on social media**.**					

Self-Efficacy

Items	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I am comfortable working with computers.					
I can learn to use most computer programs, if I am given some training.					
I can learn to use most computer programs just by reading the manuals and help documentations.					
I do not like the idea of using the Internet as a way to communicate.					
I believe that senior citizens have no use of the Internet.					

Cybersecurity Awareness

Items	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I'm aware of the Information Security concept.					
I'm aware of the Malware concept.					
I'm aware of the Antivirus software concept.					
I know that using https					

protocol is more secure than using http protocol in the URL.					
I regularly check the update of antivirus software that it used on your computer/ laptop?					

Thanks for you cooperation