Understanding Cybersecurity Awareness Among Students in Bangladesh: A Data-Driven Approach

Mehedi Hasan[1*], Maria Akter Sampa[2] & Muhammad Kawsar Mahmud[3]

[1]Registration Officer, Bangladesh Technical Education Board, Dhaka

[2]Independent Researcher, Ministry of Food, Bangladesh Secretariat, Dhaka

[3]Assistant Director (Public Relations), Civil Aviation Authority of Bangladesh & PhD Researcher, Bangladesh University of Professionals, Dhaka

[*]Correspondence Author: mastermehedi1990@gmail.com

Citation: Hasan, M., Sampa, M.A., & Mahmud, M. K. (2025). Understanding Cybersecurity Awareness Among Students in Bangladesh: A Data-Driven Approach. *Society & Sustainability*, 7 (1), 67-76. https://doi.org/10.38157/ss.v7i1.682.

Research Article

Abstract

Cybersecurity awareness is essential in the digital era, especially for university students, who are extensively engaged online and often vulnerable to cyber threats. Everyone now depends on the cyber world, increasing the space for cybercrime. Cybercrime is evolving into a severe issue in today's scenario. Cybercriminals use numerous tricks to cheat people. The cyber world has become a forte for everyone, from the government sector to people in business, school students to university students, and teenagers to adults. This kind of crime is alarmingly increasing in Bangladesh. A glomming threat has already been noted to exist in information technology. The primary purpose of this study was to explore how students keep sufficient knowledge about cybercrime to protect themselves from any unwanted situation. Primary data was collected through interviews, while secondary data was obtained by reviewing various reports, articles, and newspapers. Purposive sampling was employed to gather primary data from a diverse group of university students. Here, SPSS Version 24 has been utilized for data analysis. The study revealed mixed awareness and compliance among stakeholders in password management, browser security, and social media use, highlighting the need for better cybersecurity education. The study underscores the need for improved cybersecurity education to protect university students from growing cyber threats due to their limited awareness and risky online practices.

Keywords: Cybercrime, Cyber Security, Students

1. Introduction

Internet users are increasingly exposing themselves to security threats during their online activities. Consequently, concerns may arise regarding users' awareness of these risks and their preparedness to address any circumstances they encounter. Cybercrime has emerged as a pervasive and concerning issue in contemporary society due to the proliferation of internet usage (Mali et al., 2018). Any illegal activity involving a computer, networked device, or network is referred to as cybercrime. Cybercriminals engage in these acts to gain revenue, acquire passwords, or incapacitate computer systems or networks. Cybercrime includes ransomware attacks, email and internet fraud, identity theft, and attempts to steal financial account or credit card information. Cybercriminals may exploit personal information or corporate data for theft and subsequent sale (Brush, N.D.). The cyber realm has rapidly expanded over the past decade. Cybercriminals exploit the Internet to perpetrate various illicit activities, including virus assaults, hacking, bank fraud, software piracy, and online retail fraud. This conduct infringes upon an individual's privacy and causes

Published by *Research & Innovation Initiative Inc.,* registered with the Michigan Department of Licensing & Regulatory Affairs, United States (Reg. No. 802790777).

distress. These activities are increasing and have emerged as the world's most complex issue (Choudhary, 2020).

Cybercrime has surpassed the global illegal drug trade, with estimated losses from intellectual property and data theft reaching up to $1 trillion in 2008. Nonetheless, cybercrime is escalating significantly, with its prevalence continuously rising in Bangladesh. Cybercriminals conduct their operations through different methods, including sending threatening emails to prominent individuals, embedding pornographic content on popular websites, distributing pornography, and transmitting malicious emails to foreign diplomatic missions (Alam, 2010). Cyberspace is expanding at an exponential rate in the modern world. In addition to helping people, businesses, and governments, information and communication technologies (ICTs) also increase the scope of illegal activity (Arora, 2016). The swift advancements in computer connectivity and digital technology offer several advantages to human life, yet they are not without adverse effects, such as cybercrime.

Cybercrime represents a contemporary category of offenses utilizing internet resources, necessitating urgent and earnest attention from policymakers to safeguard the youth, who face a significant danger of victimization (Hasan et al., 2015). Cybercrime is the predominant topic of discourse in the 21st century. The global population of Internet users is rising rapidly, heightening concerns over privacy and security (Vedantu, 2023). Cybercriminals possess an extensive and always expanding domain due to the pervasive nature of the internet in many facets of our existence (Mohsin, 2022). It primarily entails utilizing the internet and computers to get an individual's private information, either directly or indirectly, and disseminating it on online platforms without the individual's consent or unlawfully, intending to tarnish the individual's reputation or inflict mental or physical harm. The proliferation of technological advancements has correspondingly accelerated the rise of cybercrime. It seriously jeopardizes individual interests, social stability, national security, and the global economy (Tuli, 2021).

Cybercrime is exerting an escalating detrimental impact in Bangladesh, primarily due to the apathy or minimal concern exhibited by individuals across many sectors regarding sharing their information online and safeguarding personal data. Cybercriminals employ phishing, smishing, and deceptive websites to acquire personal information or infiltrate an organization's computer system in pursuit of vital corporate and financial data. Individuals lack sufficient understanding of how to safeguard their personal information online. Cybercriminals have exploited this edge to capitalize on individuals' fears and anxieties. Cybercriminals disseminate information that seems credible but serves as a tactic to extract personal data from individuals. According to a report from the Bangladesh e-Government Computer Incident Response Team (BGD e-Gov CIRT), phishing, "smishing," malware, and insider threats are ranked as the third, fourth, fifth, and sixth most critical cyber dangers, respectively. Spam was identified as Bangladesh's primary cyber threat vector in 2021. Around 210.54 billion spam emails were sent every day on average worldwide in September 2021, accounting for 84.83% of all emails sent that day. Bangladesh is ranked 18th among countries as a source of spam, contributing 7.2% to the global spam volume. The significant deficiency in public knowledge is seen here. Many individuals, especially those residing in rural regions, remain unaware of the laws and regulations—their ignorance results in frequent victimization by cybercrime (Paul, 2022). A study indicates that the tribunal accepted 33 cases in 2014, with the annual number progressively rising to 1,189 by 2019. In 2020, there were 1,128 documented cases during the pandemic, and 447 cases were reported up to March of this year. Since its inception in 2013, the cyber tribunal has received almost 4,500 cases, with a rising trend in submissions, yet it has predominantly acquitted defendants (Biswas, 2021). In 2016, hackers known as "The Impact Team" compromised the dating website Ashley Madison's system, resulting in the public exposure of personal information belonging to 37 million customers. The hackers asserted that their actions were intended to reveal this practice. Many users, including several prominent figures, experienced significant embarrassment due to the incident's extensive media exposure. According to Cybersecurity Ventures, the yearly cost of cybercrime would rise from $3 trillion in 2015 to $10.5 trillion by 2025, or 15% annually. This is the biggest change in economic wealth in recorded history, endangering

Published by *Research & Innovation Initiative Inc.*, registered with the Michigan Department of Licensing & Regulatory Affairs, United States (Reg. No. 802790777).

the incentives for innovation and investment (Ahmed, 2023). Cybercrime is a significant issue that has intensified with the increasing use of computers and the internet. Cybercrime is a transnational offense with global implications. Institutions, law enforcement agencies, and other stakeholders are profoundly apprehensive regarding the complexity of cybercrime attacks and online information security. Large corporations, private individuals, and organizations with little means of self-defense are targets of these assaults. All individuals, including students, have cultivated a pronounced habit of internet usage and are particular targets for criminals (Mia, 2021).

In light of this, this study will identify how students have become aware of the effects of cybercrime and how to prevent this kind of problem. The study's main objective was to explore the level of cybercrime awareness among university students, including familiarity with common cybersecurity threats and practices.

2. Literature Review

Cybercrime primarily involves utilizing the internet and computers to acquire personal information about an individual, either directly or indirectly, and unlawfully or without consent, disseminating it on online platforms intending to harm the individual's reputation or inflict psychological or physical damage. Cybercrime refers to offenses perpetrated against individuals or groups through contemporary telecommunication networks to deliberately destroy the individual's reputation or inflict direct or indirect physical, psychological, or other forms of damage (Tuli, 2021). It impacts all sectors, including education, commerce, entertainment, and athletics. Cybercriminals, including hackers, partake in various illicit activities online, such as software piracy, virus deployment, bank fraud, online retail fraud, and numerous more offenses (Choudhary, 2020). A person who employs a computer as a means to perpetrate a crime is referred to as a cybercriminal. A cybercriminal is someone who participates in unlawful activities intended to damage others or who commits crimes associated with cybercrime (Singh et al., 2016). The most current and formidable issue in the cyber realm is cybercrime. The digital realm has proliferated swiftly during the past decade (Choudhary, 2020). Cybercrime includes a variety of techniques, such as ransomware attacks that encrypt a victim's files and demand payment for the decryption key; distributed denial of service attacks that flood a website or network with traffic, rendering it unavailable to authorized users; phishing attacks; and data breaches that give hackers access to financial data, personal information, and sensitive company information. Cybersecurity threats may result in financial loss, reputational damage, and, in certain cases, bodily injury. Enhancing the application of artificial intelligence and machine learning: These technologies enable real-time identification and reaction to cyber threats; however, they also introduce new concerns about the potential for malicious actors to exploit AI for conducting increasingly sophisticated attacks. Besides, as quantum computing advances, fraudsters will gain enhanced access to utilize it as a tool to circumvent encryption and other security protocols. As the world shifts to 5G and 6G networks, the proliferation of IoT devices will present new challenges for network security, device security, and edge security. The future of cybersecurity will increasingly prioritize technology and human-centric solutions, enhanced collaboration between the public and commercial sectors, and contemporary education. Bangladesh is evolving from a digital nation to a smart country, with cybersecurity serving as a crucial facilitator (Ahmed, 2023). As data traverses the internet swiftly, the exposure of its transmission pathways may become precarious; if unprotected, this environment can attract cyber assaults that induce disorder (Rawindaran et al., 2022). We can advance the establishment of an information-secure culture in the future by enhancing comprehension presently (Bele et al., 2014). Cybersecurity has become a significant problem and one of the most formidable challenges as digital technology evolves fast in recent years (Hong et al., 2022).

Published by *Research & Innovation Initiative Inc.,* registered with the Michigan Department of Licensing & Regulatory Affairs, United States (Reg. No. 802790777).

Cybersecurity awareness and training programs should be carefully planned to impart cybersecurity essentials since they may be a part of national security (Alqahtani, 2022). In recent years, a large number of studies have been conducted to evaluate college students' knowledge of information security threats. Students at California State University, Los Angeles' College of Business and Economics participated in a survey by Slusky and Navid (2014). The results show that the main problem with security awareness is not a lack of security knowledge but rather how pupils apply that knowledge in real-world situations. In conclusion, understanding or awareness of information security is more important than adherence. A study by Al-Janabi and Al-Shourbaji (2016) looked at the degree of cyber security expertise among Middle Eastern researchers, professors, undergraduate students, and workers in the education industry. The results show that the participants do not know enough about the importance of information security concepts and how to use them practically in day-to-day tasks. 500 students from five major cities participated in an online survey conducted by Senthilkumar and Easwaramoorthy (2017) to assess college students' understanding of cybersecurity threats in Tamil Nadu, India. According to the results, more than 70% of students were more aware of basic virus dangers and the need to use Linux systems or antivirus software (with regular updates) to defend their devices against them. The remaining pupils were vulnerable to viral infections since they did not use antivirus software. Eleven percent of them used antivirus software but neglected to update it. More than 97 percent had no idea where the infection originated.

According to Mohammed and Bamasoud (2022), cybersecurity knowledge is crucial in safeguarding the confidentiality and privacy of vital information assets. Students' understanding of cybersecurity, its hazards, and risks improves their ability to act against cybercrime, safeguarding information and technological assets to attain a secure cyberspace in alignment with Saudi Arabia's Vision 2030. Keywords: Cybersecurity. Eltahir and Ahmed (2023) indicated in their study that most undergraduate students in Sudanese higher education institutions possess inadequate cybersecurity knowledge. Subsequent analysis employing inferential statistics indicates that male students at Sudanese institutions possess marginally greater cybersecurity awareness than their female counterparts. The majority of participants advocate for the inclusion of cybersecurity education in schools and express a willingness to acquire knowledge in this field. The results indicated that students with advanced computer skills considerably differ from those with intermediate or basic computer skills in their cybersecurity practices.

The study has conceptualized some hypotheses based on the literature. These are given as follows:

H_1: Password Security is positively related to Cybersecurity Awareness.

H_2: Browser Security is positively related to Cybersecurity Awareness.

H_3: Social Media Activities are positively related to Cybersecurity Awareness.

3. Methodology

A survey methodology was employed to achieve the study's objectives and gather qualitative data on cybersecurity awareness among students at the Bangladesh University of Professionals (BUP). The survey was administered online, ensuring easy access and broad participation while maintaining data accuracy and accountability. A purposive sampling technique was used to target students with varying levels of exposure to digital platforms, ensuring a diverse representation of perspectives. This non-probability sampling method was chosen due to its effectiveness in reaching respondents actively engaged in online activities and cybersecurity practices. Additionally, online distribution facilitated the efficient collection of responses while minimizing geographical and logistical constraints.

The survey consisted of 16 items focusing on different aspects of cybersecurity, along with four demographic questions. The questionnaire was structured into three key categories (Alqahtani, 2022): (1) Password Management: Evaluating students' knowledge of secure password practices and their ability to safeguard personal information. (2) Browser Security: Assessing students' understanding of browser security features and potential threats. (3) Social media and Cybersecurity Risks: Analyzing students' awareness of security threats on social networking sites and their responses to cybercrime incidents.

Published by *Research & Innovation Initiative Inc.*, registered with the Michigan Department of Licensing & Regulatory Affairs, United States (Reg. No. 802790777).

The survey adopted a multiple-choice response format using a five-point Likert scale: Totally Agree, Agree, Neutral, Disagree, and Totally Disagree. This approach allowed a nuanced understanding of students' attitudes, competencies, and self-perceptions regarding cybersecurity. The survey was distributed among undergraduate and postgraduate students, yielding 210 responses. This sample size was deemed adequate for capturing meaningful insights into cybersecurity awareness trends within the university setting.

Employing this structured methodology, the study effectively examined students' behaviors, attitudes, and self-perceptions related to cybersecurity, contributing to a comprehensive understanding of their digital security awareness. Reliability statistics tested the reliability of the questionnaire.

Table 1: Reliability Statistics

Variable	Item	Cronbach's Alpha (Individual Variable)	Cronbach's Alpha (Overall)
Password Security	7	0.849	0.927
Browser Security	4	0.720	
Social Media Activities	5	0.847	

The generally used reliability statistics to determine if the survey questions regularly yielded trustworthy responses is the Cronbach's Alpha score for each scale and the overall measure. The usual threshold of =0.70 was used to evaluate the scales (Hair et al., 1995). Here, after considering a total of 16 items, in Table 1, it is found that the value of Cronbach Alpha coefficient of Password Security ($\alpha = 0.849$, $p<0.5$), Browser Security ($\alpha = 0.720$, $p<0.5$), and Social Media Activities ($\alpha = 0.847$, $p<0.5$) give an idea that all scales have Cronbach's alpha values of 0.70 or higher, which is acceptable for the developed Scale. It was also expected because all the questions were based on previous literature and expert opinion.

4. Results

4.1. Demographic Data

Table 2 shows more female respondents (51.9%) than male respondents. 50.5% of the respondents were 26 or older, while 49.5% were between 20 and 25. The majority of students in this survey (87.1%) have a bachelor's degree as their highest level of education. According to computer proficiency, most respondents (51.9%) are at a starting level, with intermediate users (29.5%) coming in second.

Table 2: Distribution of research respondent demographic data (n = 210)

Variable	Category	Number	Percentage (%)
Gender	Male	101	48.1
	Female	109	51.9
Age	20-25	104	49.5
	26 and above	106	50.5
Education	1st Year	35	16.7
	2nd Year	51	24.3
	3rd Year	70	33.3
	4th Year	27	12.9
	Masters	27	12.9
Computer Skill	Beginner	109	51.9
	Intermediate	62	29.5
	Advance	39	28.6

4.2. Description of the Independent Variables Used

4.2.1. Password Security

The data reveals varying attitudes towards password management and security practices. A notable portion of respondents (33.3%) are neutral about creating strong passwords with 12 characters, but 41% (totally disagree and disagree combined) lean towards not following this practice. Similarly, there is ambivalence

regarding periodic password changes, with 34.3% neutral and almost 40% in disagreement. Reusing old passwords is also contentious, with 49.5% disagreeing, though a smaller group (24.2%) agrees or strongly agrees. Opinions on using a single secure password for multiple accounts are mixed, with 37.6% disagreeing and 31.9% neutral, indicating a reluctance to embrace this practice fully. Besides, 33.3% of respondents are neutral about keeping a passcode for every webpage and account since it is inconvenient. A majority (50.5%) strongly disagree with sharing passwords, suggesting some awareness of security risks. However, the high neutrality around Two-Factor Authentication (29.5%) signals a potential gap in its adoption despite significant disagreement (38.1%) about not using it where required. These results indicate a lack of consistency in security practices, with many users either uncertain or unwilling to adopt stronger safeguards like password complexity, periodic changes, or 2FA usage.

Table 3: Password Security

Question	*Totally Disagree*	*Disagree*	*Neutral*	*Agree*	*Totally Agree*
Passwords consist of 12 characters, including a combination of letters, numerals, and symbols.	16.7%	24.3%	33.3%	12.9%	12.9%
Periodically update your password.	18.6%	20.5%	34.3%	18.1%	8.6%
Utilize passwords that have been previously used to generate new passwords whenever necessary.	28.1%	21.4%	26.2%	17.1%	7.1%
Utilize a singular safe passcode for all websites and logins.	18.1%	19.5%	31.9%	20%	9.5%
Maintaining a distinct, lengthy, robust passcode for each website and account is impractical.	22.4%	14.8%	33.3%	17.1%	12.4%
I am willing to share my passwords with my buddies.	50.5%	14.3%	21.4%	7.6%	6.2%
In the right place, I use Two-Factor Authentication (2FA).	38.1%	20.0%	29.5%	9.0%	3.3%

4.2.2. Browser Security

The data reveals varying attitudes toward web browser maintenance and privacy practices. Most respondents (43.3%) totally disagree that web browsers should be updated regularly, while 16.2% agree or totally agree, suggesting a significant reluctance to embrace updates. Similarly, while avoiding third-party extensions is somewhat polarized, with 26.7% totally disagreeing and 9.5% totally agreeing, 45.2% are either neutral or disagree to some degree, indicating mixed awareness of extension risks. Interestingly, regular examination of privacy controls garners the most neutrality (33.3%), with nearly an equal distribution of opinions across agree and disagree categories, highlighting uncertainty or indifference towards managing privacy settings. Meanwhile, 37.6% totally disagree with checking browsing history for unusual activity, further reflecting a prevalent disinterest in proactive security measures. Overall, the data suggests a need for greater awareness and user education regarding browser security and privacy best practices.

Table 4: Browser security

Question	Totally Disagree	Disagree	Neutral	Agree	Totally Agree
Browsers should be updated periodically.	43.3%	19.0%	21.4%	12.9%	3.3%
Avoid installing extensions from third-party websites.	26.7%	20.5%	25.7%	17.6%	9.5%
Check the browser's privacy settings often.	22.4%	14.8%	33.3%	17.1%	12.4%
Investigate the browsing history for any anomalous activities.	37.6%	21.4%	26.7%	10%	4.3%

4.2.3. Social Media Activities

The data presents varying attitudes toward privacy and safety on social networking sites. A significant proportion of respondents show caution when it comes to publishing private photographs, with 34.8% either disagreeing with or totally disagreeing with the practice, though 40% remain neutral. Similarly, 27.2% of respondents disagree with accepting invitations from outsiders, while 40% stay neutral, indicating hesitance toward unfamiliar interactions online. Regarding posting one's current location, 36.2% expressed

Published by *Research & Innovation Initiative Inc.*, registered with the Michigan Department of Licensing & Regulatory Affairs, United States (Reg. No. 802790777).

disagreement, though 35.7% adopted a neutral stance. The majority also exhibit caution regarding sharing personal information, with 31% disagreeing and 37.6% staying neutral. However, respondents seem to acknowledge the importance of safety, as a substantial 42.9% agree or totally agree on the need to report dangerous or questionable conduct on social networks. While many remain neutral, a considerable portion displays concerns about privacy and personal safety, reflecting apprehension over the risks of oversharing online.

Table 5: Social media activities

Question	Totally Disagree	Disagree	Neutral	Agree	Totally Agree
Sharing private photos on social media is fine.	18.1%	16.7%	40%	14.8%	10.5%
It appears acceptable to accept invitations from strangers.	14.8%	12.4%	40%	21.%	11.4%
There is no issue with sharing one's current location on social media.	22.4%	13.8%	35.7%	20.5%	7.6%
Adding personal information on social media is fine.	14.8%	16.2%	37.6%	19.5%	11.9%
Learn how to report dangerous or dubious behavior on social media.	12.4%	11.9%	32.9%	24.8%	18.1%

4.3. Correlation & Test of Hypotheses

Table 6 displays the correlations between the variables. Verifying the correlations among dimensions is essential before conducting any multiple regression analysis. The table shows that the variables—password Security, Browser Security, and Social Media Activities—positively correlate with Cybersecurity Awareness, with all correlations being statistically significant at the 1% level.

Table 6: Correlation Coefficient among the variables

Correlations					
		PS	BS	SMA	CS
PS	Pearson Correlation	1			
	Sig. (2-tailed)				
BS	Pearson Correlation	.847**	1		
	Sig. (2-tailed)	.000			
SMA	Pearson Correlation	.763**	.694**	1	
	Sig. (2-tailed)	.000	.000		
CS	Pearson Correlation	.651**	.643**	.593**	1
	Sig. (2-tailed)	.000	.000	.000	
**. Correlation is significant at the 0.01 level (2-tailed).					

Table 7: Results of the hypothesis

Hypothesis	Path	Value of r	Standardized coefficients (β)	t Statistic	P-value	Decision
H_1	Password Security > Cybersecurity Awareness	0.651	0.772	12.379	.000[b]	Significant
H_2	Browser Security > Cybersecurity Awareness	0.643	0.739	12.093	.000[b]	Significant
H_3	Social Media Activities > Cybersecurity Awareness	0.593	0.660	10.629	.000[b]	Significant

Table 8 shows that the p-value is less than 0.00. That means the null hypothesis is rejected at a 5% significance level. So, it can be concluded that Password Security is positively related to Cybersecurity awareness.

Table 8: Significance test (ANOVA)

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	99.254	1	99.254	153.239	.000[b]
Residual	134.723	208	.648		
Total	233.976	209			
a. Dependent Variable: CS_Total					
b. Predictors: (Constant), PS_Total					

Published by *Research & Innovation Initiative Inc.,* registered with the Michigan Department of Licensing & Regulatory Affairs, United States (Reg. No. 802790777).

Table 9 shows that the p-value is less than 0.00. That means the null hypothesis is rejected at the 5% significance level. So, it can be concluded that Browser Security is positively related to Cybersecurity Awareness.

Table 9: Significance test (ANOVA[a])

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	96.594	1	96.594	146.246	.000[b]
Residual	137.382	208	.660		
Total	233.976	209			
a. Dependent Variable: CS_Total					
b. Predictors: (Constant), BS_Total					

Table 10 shows that the p-value was less than 0.00. That means the null hypothesis is rejected at the 5% significance level. So, it can be concluded that Social Media Activities are positively related to Cybersecurity Awareness.

Table 10: Significance test (ANOVA[a])

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	82.359	1	82.359	112.985	.000[b]
Residual	151.618	208	.729		
Total	233.976	209			
a. Dependent Variable: CS_Total					
b. Predictors: (Constant), SMA_Total					

5. Discussions

Cybersecurity awareness among students is critical in ensuring digital safety in an increasingly interconnected world. This study highlights the prevailing attitudes and behaviors regarding cybersecurity practices, revealing a complex interplay between knowledge, perception, and application of security measures. While some students exhibit a basic understanding of cybersecurity principles, inconsistencies in adopting best practices suggest a gap between awareness and implementation.

One key area of concern is password security, where varying levels of commitment to creating strong and unique passwords indicate a need for further education. Many individuals may recognize the importance of password security but fail to take proactive measures, leaving their accounts vulnerable to potential breaches. Similarly, reluctance or indifference toward Two-Factor Authentication suggests that additional awareness efforts are necessary to promote this critical security feature.

Another challenge lies in browser security and privacy practices. Regular software updates, privacy settings management, and vigilance against potential threats are fundamental to maintaining a secure online presence. However, a general hesitancy to embrace these measures implies that misconceptions or a lack of knowledge may hinder the adoption of effective security protocols. Addressing these gaps through structured educational initiatives could improve digital hygiene among students.

Social media platforms present another dimension of cybersecurity risks, as they are commonly used for communication, networking, and information sharing. While some individuals demonstrate caution regarding privacy settings and information sharing, many remain uncertain about the potential risks associated with online interactions. Encouraging responsible social media practices and fostering an understanding of digital footprints could help mitigate threats related to identity theft, phishing, and cyberstalking.

The study underscores the necessity of enhancing cybersecurity education and awareness programs. Institutions, educators, and policymakers must work collaboratively to bridge the gap between knowledge and practice by integrating cybersecurity training into academic curricula and extracurricular activities. By fostering a culture of digital responsibility, students can develop the skills and awareness needed to navigate the digital landscape safely and effectively.

Ultimately, cybersecurity awareness should not be viewed as an isolated concern but as an essential component of digital literacy. Strengthening proactive security behaviors, promoting critical thinking about

Published by *Research & Innovation Initiative Inc.*, registered with the Michigan Department of Licensing & Regulatory Affairs, United States (Reg. No. 802790777).

online risks, and encouraging responsible digital engagement will contribute to a more secure cyber environment for students and society as a whole.

6. Conclusions

This study elucidates the cybersecurity behaviors and attitudes of young, educated individuals with novice computer abilities, emphasizing password management, browser security, and social media utilization practices. The findings indicate varying degrees of compliance with recommended security protocols, with certain respondents adhering to secure password practices—such as formulating robust, unique passwords and regularly changing them—while others exhibited indifferent or dismissive attitudes towards these fundamentals. Moreover, while most participants refrain from exchanging passwords, a limited number utilize two-factor authentication, an essential measure for online security. Browser security measures are also neglected since students rarely change privacy settings or scrutinize surfing activity for anomalous behavior. Social media behaviors indicate additional concerns, such as the habitual sharing of personal information, accepting friend requests from unfamiliar individuals, and a pervasive lack of prudence in public disclosures.

Based on the above discussion, the study offers a few recommendations. Tailored education initiatives should be designed and implemented to strengthen cybersecurity awareness among university students, focusing on practical skills and best practices. Monthly workshops and seminars with cybersecurity experts can help keep students informed about emerging threats. Universities should promote strong, unique passwords by providing clear guidelines and tools for effective password management. Integrating cybersecurity topics into academic curricula will ensure that students understand the relevance of security in their respective fields. Regular assessments of students' cybersecurity knowledge can help identify gaps and refine educational strategies. Additionally, raising awareness about privacy settings and safe social media practices is essential to minimize risks related to personal data exposure.

7. Limitations and Future Research

This study has specific limitations that require consideration. The literature suggests that a comprehensive study is necessary to address the issue of cybersecurity. Based on a limited sample size of 210 and confined to a narrow geographic area, this study may not fully represent Bangladesh's broader context. Future research could expand the scope by incorporating additional domains and employing qualitative methods for deeper insights. While regression analysis was used to examine variable relationships, further studies may apply supplementary statistical techniques, using this research as a foundational reference.

Authors' Contribution: Mehedi Hasan contributed to the writing of the Abstract, Introduction, Methodology, and Literature Review and identified the Research Gaps and Limitations and Future Research. Maria Akter Sampa was responsible for drafting the Results, Discussion, Conclusion, and Recommendations sections. Muhammad Kawsar Mahmud assisted with the Literature Review, identified the Research Gaps, Prepared the Questionnaire, and collected Data. All authors' collective efforts ensured the manuscript's quality and comprehensiveness.

Conflict of Interest: The authors declare no conflict of interest.

REFERENCES

Ahmed (2023). *Cyber security threats to Smart Bangladesh*. The Daily Star, Retrieved from https://www.thedailystar.net/: https://www.thedailystar.net/business/economy/news/cyber-security-threats-smart-bangladesh-3225711

Alam, M. (2010). *Cybercrime in Bangladesh: Implications and response strategy*. *NDC Journal*.

Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cybersecurity awareness in the educational environment in the Middle East. *Information Knowledge Management*, 15, 1650007. https://doi.org/10.1142/S0219649216500076

Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences, 12*(5), 2589. https://doi.org/10.3390/app12052589

Arora, A. (2016). Exploring and analyzing internet crimes and their behaviors. *Perspectives in Science*, *8*, 540–542.

Biswas (2021). *Cybercrime cases rise in Bangladesh, but suspects are mostly acquitted*. Retrieved from https://bdnews24.com/bangladesh/cybercrime-cases-rise-in-bangladesh-but-suspects-are-mostly-acquitted#:~:text=People%20filed%201%2C128%20cases%20amid,were%20acquitted%20during%20charge%2Dframing.

Brush (N.D). *cybercrime.* Retrieved from https://www.techtarget.com/searchsecurity/definition/cybercrime

Choudhary (2020). Cyber Crime Awareness Among Higher Education Students from Haryana With Respect to Various Demographical Variables. *PalArch's Journal of Archaeology of Egypt / Egyptology*, 7(17), 14454- 14461

Eltahir, M. E., & Ahmed, O. S. (2023). Cybersecurity awareness in African higher education institutions: A case study of Sudan. *Information Sciences Letters*, *12*(1). https://digitalcommons.aaru.edu.jo/isl/vol12/iss1/13

Hasan, H., Rahman, R. A., Sulaiman, A., & Harun, M. (2015). Perception and awareness of young internet users towards cybercrime: Evidence from Malaysia. *Journal of Social Sciences, 11*(4), 395–404. https://doi.org/10.3844/jssp.2015.395.404

Hong, W. C. H., Chi, C., Liu, J., Zhang, Y., Lei, V. N., & Xu, X. (2022). The influence of social education level on cybersecurity awareness and behavior: a comparative study of university students and working graduates. *Education and Information Technologies*, 28(1), 439–470. https://doi.org/10.1007/s10639-022-11121-5

Bele, J. L., Dimc, M., Rozman, D., & Jemec, A. S. (2014). Raising awareness of cybercrime: The use of education as a means of prevention and protection. *International Association for the Development of the Information Society*.

Mali et al. (2018). Analysing The Awareness of Cyber Crime and Designing A Relevant Framework With Respect to Cyber Warfare: An Empirical Study. *International Journal of Mechanical Engineering and Technology (IJMET).* 9 (2), 110–124.

Mia, A. (2021). Cybercrime and its impact in Bangladesh: A quest for necessary legislation. *International Journal of Law and Legal Jurisprudence Studies*, *2*(4).

Mohammed, A., & Bamasoud, M. (2022). The impact of enhancing awareness of cybersecurity on university students: A survey paper. *Journal of Theoretical and Applied Information Technology, 100*(5), 4756–4766.

Mohsin (2022). *How senior citizens can remain safe from cybercrimes*. Retrieved from https://www.thedailystar.net/: https://www.thedailystar.net/tech-startup/news/how-senior-citizens-can-remain-safe-cybercrimes-3107931

Paul, S (2022, September 19). *Bangladesh is at serious risk of cyber crimes*. Retrieved from https://www.dhakatribune.com/op-ed/2022/09/19/bangladesh-is-at-serious-risk-of-cyber-crimes

Rawindaran, N., Jayal, A., & Prakash, E. (2022). Exploration of the Impact of Cybersecurity Awareness on Small and Medium Enterprises (SMEs) in Wales Using Intelligent Software to Combat Cybercrime. Computers, 11(12), 174. *MDPI* AG. Retrieved from http://dx.doi.org/10.3390/computers11120174.

Singh, O., Gupta, P., & Kumarŧ, R. (2016). A Review of Indian Approach towards Cybersecurity. Retrieved on April 14, 2019 from https://bit.ly/2INZeEy

Slusky, L., & Partow-Navid, P. (2014). Students' information security practices and awareness. *Journal of Information Privacy and Security*, *10*(1), 3-26. https://doi.org/10.1080/15536548.2012.10845664

Tuli (2021). A Study on Cyber Crime and its Legal Framework in India. *International Journal of Law Management and Humanities*. 4 (2), 493 – 504.

Vedantu (2023). *Cyber Crime Essay*. Retrieved from https://www.vedantu.com/: https://www.vedantu.com/english/cyber-crime-essay.