Scientific Research Publishing

Advances in Journalism and Communication, 2022, 10, 70-80
https://www.scirp.org/journal/ajc
ISSN Online: 2328-4935
ISSN Print: 2328-4927

Data Privacy on the Internet: A Study on Awareness and Attitudes among the Students of the University of Chittagong in Bangladesh

Madhab Chandra Das

Department of Communication and Journalism, University of Chittagong, Chattogram, Bangladesh
Email: madhabdas@cu.ac.bd

How to cite this paper: Das, M. C. (2022). Data Privacy on the Internet: A Study on Awareness and Attitudes among the Students of the University of Chittagong in Bangladesh. *Advances in Journalism and Communication, 10,* 70-80.
https://doi.org/10.4236/ajc.2022.102006

Received: March 7, 2022
Accepted: May 4, 2022
Published: May 7, 2022

Abstract

Almost every nation in the world, including Bangladesh, has seen remarkable growth in internet use over the previous decade. It is a good sign but not safe because the users are concerned about their data security. Generally, it can be said that internet users love to share the information they like the most without any sort of thought. This article aims to find out the university students' attitudes and awareness regarding data privacy and cybersecurity. More specifically, the researcher conducted an online survey using Google Form to apprehend the level of understanding and practice regarding data security among the students of the University of Chittagong, a state-owned university in Bangladesh. A semi-structured questionnaire was used to obtain the data needed to meet the aims. The data analysis was carried out using SPSS, version 25. Participants in this research were 180 students from three distinct faculties at the University of Chittagong in Bangladesh. Through the analysis of the survey findings, the researcher hopes to measure the respondents' knowledge, skills, and attitudes towards digital technology and its privacy issues. This article also aims to check the target audience's cybersecurity awareness and willingness to practice it personally. Every day, the dependence on internet use increases proportionately with the rise of ICT and digital platforms. It has become essential to understand data privacy and cybersecurity issues in this age of cutting-edge technology. As a result, the researcher chose university-level students to assess their cybersecurity and data protection awareness and practice while using digital technologies in their daily lives.

Keywords

Personal Information, Cybercrime, Victim, Harassment, Cybersecurity

1. Introduction

Data are always considered the fuel of digital platforms. In line with the modern world, a significant portion of the youth of Bangladesh, especially the younger generation at the university level, use ICT (Information and Communication Technology) for various purposes. Because of the increased prevalence of internet access, everything from purchasing to banking is now just a click away. On the other hand, cybercriminals are taking advantage of the internet platform, engaging in various illegal operations such as scamming, phishing, hacking, and stealing personal information (Babu, 2021). According to a study, Bangladesh has grown into a regional hub for new media audience engagement in South Asia, with more than 125.46 million internet users and 178.61 million mobile phone users (BTRC, 2021).

Additionally, Bangladesh has its perspective plan with Vision 2041 to transform the country into a developed one with a constitutional mandate to establish a fully-fledged digital society. The use of social media such as Facebook, YouTube, Instagram, Tik-Tok, Imo, Snapchat, Telegram, WhatsApp, etc., among Bangladeshi youth is growing faster than ever before. Internet users frequently install different types of mobile apps to stay connected and get informed. They have to give some of their personal information to run the apps or use the digital platforms. And cybercriminals take this opportunity to materialize their ill intentions. In Bangladesh, both state-owned and private enterprises are becoming targets of cyber-attacks that might have detrimental impacts on the lives of internet users. Thousands of incidents are being noticed every day because most users' data is not protected. Other nations' conditions are almost identical and are much more severe and terrible in some cases. Now it is high time to increase awareness about personal data privacy and ensure the data security of its users.

As most of the users in Bangladesh are not conscious and aware of the value of personal data, taking steps at the government level has become a must to ensure the best and safest use of ICT. This article will examine young students' levels of awareness and attitudes toward data security. It will also be helpful for policymakers to initiate measures at the government level.

2. Operational Definition

Cybercrime: According to the ICT Act (2006), all crimes produced electronically or computer-based are considered cybercrimes.

Data privacy: It refers to the safeguarding of personal information against unauthorized access and the capacity of people to control who has access to personal data.

Data security: It is the practice of preventing unwanted access to confidential information. Encryption, access limitations (physical and digital), and much more are included within this category of cybersecurity strategies.

Personal data: Bangladesh has entered the data protection arena by implement-

ing the Digital Security Act (2018). Personal data is defined in Section 26 of the Digital Security Act as "identification information." Section 26 states that "clear permission or approval" be sought from an individual prior to collecting, marketing, keeping, maintaining, providing, or reusing his or her personal information.

Phishing attack: Phishing is a sort of criminality that employs a fake email or link to deceive the receiver into thinking the communication is authentic. If the victim falls for the ruse, they will wind up clicking a malicious attachment or downloading a harmful file, jeopardizing their essential personal information protection.

3. Research Objectives

General Objective

The study's primary objective is to examine to what extent university students are aware of their online data and what attitudes they show towards their data privacy.

Specific Objectives

1) To highlight the current scenario of cybercrimes in Bangladesh.

2) To evaluate the youth's knowledge of the cyber environment.

3) To discuss the increasing frequency of cybercrimes in Bangladesh.

4) To identify the type of action taken by the victim of cyber harassments.

5) To recommend some courses of action for the Bangladesh government to incorporate.

4. Literature Review

Recently, hackers disclosed the personal information of 533 million Facebook users worldwide, including 3 million (3,816,339) Bangladeshis. These statistics, published in a low-key cybersecurity forum, remain publicly available.

The exposed information includes, but is not limited to, a user's Facebook ID number, profile names, email addresses, primary location data, gender, and work status—basically any information that a person posts in the information part of their profile (Rahman, 2021).

Researchers Farida Chowdhury, Sadia Sultana, and Mahruba Sharmin Chowdhury examined how Bangladeshi women who use social media express their concerns about safety and privacy online. In their research report, 66% reported that they do not upload or share their ideas or photographs on a regular basis, which indicates that female users are not comfortable or eager to do so. Even if they publish anything, 90.1% do not post it publicly. Privacy and security are the main reasons for this (Chowdhury et al., 2021). In another study in Bangladesh, Ahmed et al. (2017) found that 36.8% of users reported being harassed, and 78.9% reported encountering unexpected circumstances that may be classified as harassing. According to the survey's results, 84.2 percent of Facebook users have been harassed by those with whom they are connected on the social networking site. Around 27% of abuse originated from unknown people who met for the first time

on Facebook. Furthermore, 10.5 percent of the harassment was perpetrated by unidentified individuals, while recognized individuals perpetrated 5.3 percent.

In a 2020 survey on cybersecurity awareness, 85% of students and 95% of professors at a Sudanese college agreed to share their personal information, such as passwords, with IT staff. It was discovered in this study that almost three-quarters of those who completed the research survey said they have been victims of cybercrime or have had the unpleasant experience of having their personal information stolen while using social media. However, three-quarters of them could use a variety of capital, lowercase, figures, and special characters at some point in their passwords. The typical person's degree of cybersecurity knowledge is relatively low. Compared to students, faculty members outperformed them in terms of knowledge and skillsets, with 54 percent and 46 percent of the total, respectively (Elradi et al., 2020). Research published in the Turkish Journal of Education by Mehmet Tekerek and Adem Tekerek found that female students had a higher level of data security awareness than male pupils (Venter et al., 2019). Additionally, 90% of software in Bangladesh is unlicensed, which increases the danger of cybercrime due to its poor security (Babu, 2021).

5. Materials and Methodology

During the pandemic, online platforms have emerged as a powerful communication tool worldwide, especially in the education sector. As all the users of academic institutions had to use ICT, we liked to see the level of awareness about data security. For this reason, we have randomly chosen students below or up to 22 years old from three different faculties of the University of Chittagong, a state-owned university in Bangladesh. These are the Faculty of Social Sciences, the Arts and Humanities, and the Faculty of Business Studies.

We used a Google Form to create a survey question covering several questions about internet usage and cybersecurity concepts. We collected replies from the students of the randomized faculties mentioned above. Our findings have been categorized here into four sections. **Figure 1** and **Figure 2** show the demographics of the respondents, while **Table 1** and **Table 2** show how well respondents knew and used cybersecurity, respectively. This survey was done among 180 students. In other words, sixty students from each faculty participated in this survey.

The demographics of participants are depicted in the first and second figures. Cybersecurity awareness and practice levels are illustrated in the first and second tables. The first and second figures asked two questions to draw demographic data. In the first table, we asked ten questions to find out the awareness level, and in the second table, we asked seven questions to see the cybersecurity awareness practice level of the respondents.

6. Results

Figure 1 shows that, among all the respondents, 61% were women, and 39% were men. **Figure 2** illustrates that 55% of participants were below 22 years old, while 55% were up to 22 years old.

Table 1. Awareness level of the respondents regarding cybersecurity and data privacy.

Variables	Categories	Percentage
Type/s of social media most commonly used	Facebook	93.5
	Instagram	6.5
Aware of security features offered by social media providers	Yes	87.1
	No	9.7
	No idea	3.2
Current social media account profile status	Private	51.6
	Public	45.2
	No idea	3.2
Possibility of risk associated with having a public social media profile	Yes	74.2
	No	22.6
	Do not care	3.2
Understand how to browse social networking sites' system settings and configure the available security choices	Yes	64.5
	No	35.5
Experienced as a target of a cyber threat, a breach of security, or a violation of privacy	Yes	74.2
	No	25.8
Understanding level of phishing attacks	Yes	64.5
	No	35.5
Installing app may hamper your personal data security	Agree	77
	Disagree	23
Use of VPN	Yes	74.2
	No	22.6
	No idea	3.2
Concerns about the usage of users' data by social media platforms	Yes	67.7
	No	32.3

Table 2. Practice level of the respondents as to cybersecurity and data privacy.

Variables	Categories	Percentage
Check emails regularly to see if there have been any unusual login attempts	Yes	45.1
	No	48.4
	Not applicable	6.5
Assure HTTPS connections when transmitting sensitive data online	Yes	38.7
	No	41.9
	Not applicable	19.4

Continued

Caution about what kind of information is being disclosed	Yes	71.0
	No	19.4
	Not applicable	9.6
Logging off accounts after use	Yes	19.5
	No	75.5
	No idea	5
Use a strong password and a password manager to keep information safe	Yes	53
	No	47
Report to the law enforcers in the case of harassment	Yes	20.5
	No	79.5
The tendency to keep software and devices updated	Yes	100

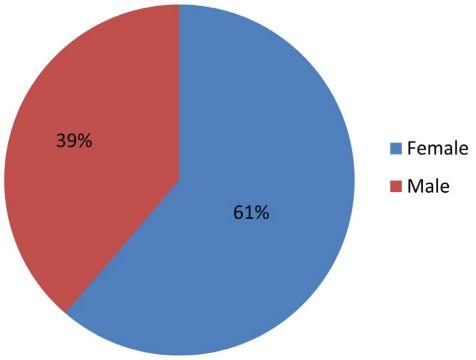

Figure 1. Gender of the respondents.

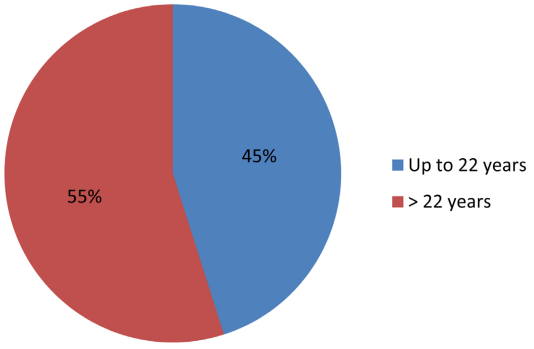

Figure 2. Age of the respondents.

Table 1 shows the cybersecurity awareness level among the respondents. Though Facebook, Snapchat, Twitter, Instagram, LinkedIn, etc., are the most popular social media platforms worldwide, it is interesting that 93.5% of the respondents use Facebook while only 6.5% use Instagram. But among the respondents, none used the other social media platforms. We asked respondents how familiar they were with the security features provided by social media platforms.

As per the received data, we can see that 87.1% of respondents are aware of the security features or systems of the social media providers, while 9.7% are not aware of it, and 3.2% of them have no idea about it. Among the respondents, 51.6% have kept their profile status private, while 45.2% of respondents have kept their profile status public. At the same time, the rest, 3.2% of respondents, have no idea about their profile status though they use social media as usual. The respondents were also asked about the potential risk of having a public social media profile. According to the answers, 74.2% of respondents think it is risky to keep their profile status public, while 22.6% think it is not risky, and the remaining 3.2% do not care about the risk. 64.5% of the respondents answered that they have knowledge of the navigation system of social media settings and the available security options. In comparison, the remaining 35.5% of respondents said they do not have any knowledge regarding the issue.

Almost three-quarters of the respondents (74.2%) answered that they have become victims of cybercrime or have faced the bad experience of losing their privacy on social media. In comparison, the rest of the participants (25.8%) answered "no" to the same issue. 64.5% of students responded that they knew about the phishing attacks, and the rest, 35.5%, did not know this term. Approximately three-quarters (77%) of the respondents agreed that installing mobile applications may hamper their data security, and the rest (23%) of the respondents do not think so. Among the responding students, 74.2% answered that they use VPN, 26.6% answered "no," and the rest, 3.2%, had no idea about it or had no scope to use it. 67.7% of students are concerned about using their data on social media platforms, while 32.3% are not concerned about this issue.

Table 2 illustrates the cybersecurity awareness practice level among the respondents. In order to search for unusual login attempts, 45.1% of individuals check their emails regularly, 48.4% do not, and 6.5% are completely unaware that this is an option. 38.7% of participants ensure HTTPS connections when transmitting sensitive data online, 41.9% do not ensure it, and 19.4% of the respondents are entirely unaware of it. Before disclosing any information, 71% of participants ponder what information they could be sharing with others (vacation locations and durations, residence or work address), while 19.4% of participants do not give it a second thought, and 9.6% are entirely unaware of it. In the case of logging off accounts when used, 75.5% of participants do not log off from their accounts after finishing their tasks, 19.5% log off after completing tasks, and the rest, 5%, are unaware of the log-off. Just over a half (53%) of those who took part in the survey used strong passwords and used a password manager, with the remaining 47% not aware of what they were doing. However, 100% of participants responded that they tend to keep software and devices updated on a regular basis.

7. Discussion

Pathao, a ride-sharing platform developed in Bangladesh, has recently been crit-

icized for suspicions of unlawful access to customers' SMS and phone numbers. Additionally, this incident sparked a significant debate in Bangladesh on the security of personal data (Moniruzzaman, 2019). According to a Cyber Crime Awareness Foundation report, social media account hacking has increased from 13% in 2019 to 28% in 2021 (Khan & Saad, 2021). So, we should not disclose sensitive personal information on social media. The Bangladesh government passed the Digital Security Act 2018 for the first time in the country's history to protect the country's digital security and set rules for how to find and respond to cybercrime. Before passing this law, no one in Bangladesh was responsible for accessing or disclosing their personal information. A provision for the protection of personal information is also included in that Act. Identity information is defined in this statute as "any external, biological, or physical information" that may be used to identify an individual or a system. Biometric data such as fingerprints, passport numbers, account numbers, driver's license numbers, and e-TIN numbers are among the things that belong in this category. Other items that fall under this category are social security numbers and birth certificates. This article's findings say cybercrimes will be less common if nearly one-third of people learn how to keep their personal data safe. Social media account hacking has increased from 13% in 2019 to 28% in 2021, according to a report by the Cyber Crime Awareness Foundation (CCA Foundation) of Dhaka, Bangladesh. In the research report, Rashna Imam, an adviser to the organization, said that cybercrimes in Bangladesh increased alarmingly in 2019-2020. It included social media and other online accounts' hacking and information-stealing incidents. New crimes like ATM card hacking have also been identified. According to the report, instances of social media accounts and other online accounts being hacked currently stand at 28.31%, having increased nearly 13% from 2019's rate of 15.35% (The Business Standard, 2021).

According to our survey, 75.5% of participants do not log off from their accounts after finishing their tasks. Over half (53%) of participants are not careful about using a strong password and password manager. These figures show that internet users' behavior plays a beneficial role for criminals in fulfilling their targets. So, internet users should be more and more aware of their bad or wrong attitudes and behavior towards using ICT by responsible organizations like ICT providers, government and non-government bodies, volunteers, etc. Our survey gave us a picture of the cybersecurity awareness practice level of the users. Many users are unaware of the cybersecurity measures provided by their devices, social media providers, and software developers, and many are unconcerned about the issue. Most of them ignore it until they become victims. They do not know about it, even after using steps to protect themselves from cybercrimes. If internet users were aware of the vulnerabilities of cybersecurity concerns and the consequences, they would devise strategies to defend themselves. When the users are careful about protecting themselves, it will be easier for the safety authorities to find the crimes and find a good way to solve them. On social media, young women and children are being exploited, blackmailed, and bullied in unprece-

dented numbers by cybercriminals. In the seven months since its establishment, the Police Cyber Support for Women (PCSW) in Bangladesh has received at least 15,000 complaints about cybercrime against women (Haque, 2021).

Several multinational hacker groups from Eastern Europe and Asia were responsible for cyber-attacks on more than 200 Bangladeshi companies, which undermined Bangladesh's cybersecurity. Cyber and privacy dangers are now everywhere, affecting the whole network of businesses. It should come as no surprise that cyber threats have risen to the second-highest level of worry, according to the PwC Global CEO Survey 2021, which quotes different Chief Executive Officers (CEOs) from across the world. The threat of pandemics and health-related disasters ranked first on the list of dangers. As per the Bangladesh Bank's Yearly Report for the budget year 2019-20, the bank has strengthened its cybersecurity procedures (Haque, 2021).

Our survey revealed that a significant proportion (79.5%) of participants does not report any harassment, and only 20.5% of participants answered that they register harassment officially if they face any. The study shows that the number of victims is considerably high and increases rapidly over time. This study affirms that most victims do not seek help from the responsible wings. A question arises here: "why"? The study does not answer the question "why," but we can conclude that many users are still unaware of the security of their personal information. According to our findings, to overcome this situation, the government and other private employer organizations should launch more awareness-related programs and activities to make online users confident and ready not to be victims of cyberattacks.

8. Social Implications of the Study

Cybercrime is a global issue. With the passage of time, its nature has been remodeled by cybercriminals. Bangladesh, however, has reached a countable position globally after 50 years of its birth. As we move towards a developed world, we have to increase our awareness level to combat cybercrime. We found that internet users, even at the university level, lack ICT knowledge and skills, and their attitudes toward data security are not up to the mark. If this scenario is established at this level, what will be the situation in rural areas where people have little or no awareness of information and communications technology? Doing this study, we have become astonished at the silent role of the victims of cybercrimes.

However, there is no question that technological defense is superior to legal remedies in stopping high-tech crimes. Still, there is always the possibility of such security measures being destroyed since they are not permanent. This crisis requires a robust online security mechanism. As a consequence of our research, the government should take some new courses of action similar to those taken by the world's most advanced high-tech nations. The younger generation, especially university students, should be aware of the safety of their personal infor-

mation before using internet platforms or services, particularly social media.

9. Conclusion

The majority of those who fall prey to cybercrime are not conscious of their virtual security. Many victims were reluctant to register complaints against the criminals, fearing that they would be subjected to additional harassment. The example of Nila (who does not want to be identified by her actual name) is a good illustration. Using social media, she came across an expatriate who resided in the Middle East and developed a relationship with him. She eloped with that man but later discovered that the gentleman had been having an extramarital affair with another lady. After Nila ended the relationship with him, her ex-husband created fake social media profiles in her name and posted intimate images of her on them. Although Nila recorded a general diary (GD) at the police station, she chose not to file a lawsuit because she feared that if she did, her family's name would be dragged through the dirt as a result (Khan & Saad, 2021). Besides the Information and Communication Technology (ICT) Act of 2006 and the Digital Security Act (DSA) of 2018, Bangladesh does not have a law protecting against cybercrime. It has been ten years since surveillance technology has made giant leaps. The current legal system in Bangladesh cannot deal with the new issues that might arise because of rapid technological advancements (Haque, 2021).

In 2009, North Korea launched the "Korea Internet and Security Institution", a government agency formed by the merger of three of the country's previous internet technology groups. Now, this organization is working to make North Korea a more secure and modern nation in terms of internet use. India and a few other nations have also established similar institutions (Maruf et al., 2014). Though a few cyber-units are actively functioning in Bangladesh to trace, prevent, and stop cyberterrorism and cybercrime, this study also recommends that, considering the rapid increase of internet users and the intensity of cybercrime in Bangladesh, the government should form more similar organizations. However, more study is needed in this field to picture the real scenario and to set the policies, activities, and arrangements to protect the users from the touch of cybercriminals. Otherwise, we may have wealth, but we will not have peace in our lives.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

Ahmed, S., Kabir, A., Sneha, S. S. A., & Jafrin, S. (2017). Cyber-Crimes against Womenfolk on Social Networks: Bangladesh Context. *International Journal of Computer Applications, 174,* 9-15. https://doi.org/10.5120/ijca2017915407

Babu, K. E. K. (2021). Cyber Security in the Global Village and Challenges for Bangladesh: An Overview on Legal Context. In H. Jahankhani, A. Jamal, & S. Lawson (Eds.),

Cybersecurity, Privacy and Freedom Protection in the Connected World (pp. 253-267). Springer. https://doi.org/10.1007/978-3-030-68534-8_16

BTRC (2021). *Government of the People's Republic of Bangladesh.* http://www.btrc.gov.bd/site/page/347df7fe-409f-451e-a415-65b109a207f5/-

Chowdhury, F., Sultana, S., & Chowdhury M. S. (2021). Security and Privacy Perceptions among Female Online Social Media Users: A Case Study of Bangladesh. *International Journal of Security, Privacy and Trust Manage, 10,* 1-14. https://aircconline.com/abstract/ijsptm/v10n1/10121ijsptm01.html

Elradi, M. D., Altigani, A. A., & Abaker, O. I. (2020). Cyber Security Awareness among Students and Faculty Members in a Sudanese College. *Electrical Science & Engineering, 2,* 24-28. https://doi.org/10.30564/ese.v2i2.2477

Haque, E. (2021). Pegasus Controversy and Cyber Security in Bangladesh. *The Daily Star.* https://www.thedailystar.net/law-our-rights/news/pegasus-controversy-and-cyber-security-bangladesh-2143751

Khan, M. J. & Saad, M. (2021). Cybercrimes against Women Rampant. Over 15,000 Complaints of Bullying, Harassment, Blackmailing in 7 Months. *The Daily Star.* https://www.thedailystar.net/frontpage/news/cybercrimes-against-women-rampant-2113093

Maruf, A. M., Islam, M. R., & Ahamed, B. (2014). Emerging Cyber Threats in Bangladesh: In Quest of Effective Legal Remedies. *Northern University Journal of Law, 1,* 112-124. https://doi.org/10.3329/nujl.v1i0.18529

Moniruzzaman, M. (2019). Personal Data Protection in Bangladesh and GDPR. *Bangladesh Journal of Legal Studies.* https://bdjls.org/personal-data-protection-in-bangladesh

Rahman, S. (2021). 3 Million Bangladeshi Facebook Users' Personal Data Exposed during a Massive Data Leak. *The Daily Star.* https://www.thedailystar.net/toggle/news/3-million-bangladeshi-fb-users-personal-data-exposed-during-massive-data-leak-fb-2071777

The Business Standard (2021). *Social Media Hacking Increased 13% in 2 Years.* https://www.tbsnews.net/tech/ict/social-media-hacking-increased-13-310057

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber Security Education Is as Essential as "The Three R's". *Heliyon, 5,* e02855. https://doi.org/10.1016/j.heliyon.2019.e02855