Determining Cybersecurity Awareness and Human-Cyber Behaviour in Bangladeshi Women: Addressing Factors, Risks and Overcoming Knowledge Disparities.

by

Maliha Tasnim
21301462
Maisha Tasnim
21301460
Samsad Laila
21301253
Tanzuma Tabassum
23241056
Seham Al Haque
21201395

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering
BRAC University
February 2025

Declaration

It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name & Signature:

Maliha Tasnim

21301462

Maisha Tasnim

21301460

Samsad Laila

21301253

Tanzuma Tabassum

23241056

Seham Al Haque

21201395

Approval

The thesis/project titled "Determining Cybersecurity Awareness and Human-Cyber Behaviour in Bangladeshi Women: Addressing Factors, Risks and Overcoming Knowledge Disparities." submitted by

1. Maliha Tasnim (21301462)
2. Maisha Tasnim (21301460)
3. Samsad Laila (21301253)
4. Tanzuma Tabassum (23241056)
5. Seham Al Haque (21201395)

Of Fall, 2024 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on February 3, 2025.

Examining Committee:
Supervisor:
(Member)

Dr. Farida Chowdhury

Professor
Department of Computer Science and Engineering
BRAC University

Program Coordinator:
(Member)

Md. Golam Rabiul Alam

Professor
Department of Computer Science and Engineering
BRAC University

Departmental Head:
(Chair)

Dr. Sadia Hamid Kazi

Chairperson and Associate Professor
Department of Computer Science and Engineering
BRAC University

Ethics Statement

All the necessary measures were considered to ensure the research process adhered to ethical standards, covering the following steps.

1. **Informed Consent:** Participants involved in the surveys and interviews were properly briefed about the research objectives and intended for the use of their data. Participants' involvement was completely voluntary. Consent was obtained through a consent form before collecting data. For the underage participants, parental oral consent was taken for interviews and school authorities' permission was obtained for the survey.

2. **Data Confidentiality and Anonymity:** All personal and sensitive data were collected anonymously ensuring participants' privacy. Necessary measures are taken to securely store their data, ensuring that no identifying details were disclosed at any part of this research.

3. **Compliance with Applicable Laws and Regulations:** This research was carried out in full compliance with legal requirements from the institutional authority and guidelines. No part of the data collection or analysis process has violated national or international data protection laws and regulations.

4. **Research Integrity:** The authors confirm that all data presented is valid and accurate. All findings are consist of no fabrication or falsification. No plagiarism was involved in conducting or presenting this research. To ensure transparency and credibility, proper citations have been provided for all external references.

By adhering to these ethical principles, this research ensures to maintain the proper standards of ethical integrity.

Abstract

In the era of advancement where technology is widespread, cybersecurity has an indispensable impact on its ongoing advancement. The cybersecurity practices of women in Bangladesh and its consequences are critically vulnerable. Cybersecurity awareness uncovers emerging threats in responding to changing circumstances. In this research, we comprehend cybersecurity awareness knowledge across different demographics of Bangladeshi women. By identifying human cyber behaviour and situational factor, practice and prospective risks this study addresses women's perceptions, knowledge and response strategies regarding cybersecurity awareness. Investigating through qualitative and quantitative approaches, this research analyzes three groups of women (High School students, University students and Working women). Through quantitative analysis, a large-scale survey (n=1,202) is conducted to analyze the awareness of women. Then we conducted a semi-structured interview (n=30) with all three groups to gather the in-depth study of women's human behaviour and situational factors that lead to risky cyber decisions and cyber threats. This study investigates prevalent cybersecurity risk and threat encountered by women. The research findings reveal that women's exposure to cyber threats is not merely a consequence of inadequate knowledge but also influenced by behavioural pattern and situational vulnerabilities. Our research unveils the substantial barriers that leave women digitally insecure. Finally, this research proposes a framework and practical suggestions to improve women's cybersecurity awareness knowledge and provide a roadmap for safe digital usage.

Keywords: Cybersecurity, Awareness, User behaviour, Privacy, Design Intervention, Security-Threats, Cybersecurity habits.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Security has become an important aspect of our everyday life and a mission essential function for all business either virtual or physical. We want a safe place and have rights to defend it but at times we are unaware of the threats that surround us and how to defend ourselves. Hence, we need cybersecurity awareness to prevent such incidents from occurring [77]. According to Seemma et al. [57] the security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of cyber security. Cybersecurity is a young field of practice whose importance and prominence has grown exponentially over the last two decades. Even so, the number of major cybersecurity incidents continues to be a concern [62]. Cybersecurity is important as our lives become more interconnected by technology, to safeguard both personal and organizational data because cyber threats are ever evolving; we remain vulnerable unless we constantly remain in cyber practice. We need to have such a culture of cybersecurity awareness that we can all safely move around in the digital world and build a safer, more secure future for everyone. Cybersecurity awareness involves being mindful of cybersecurity in day-to-day situations. Being aware of the dangers of browsing the web, checking email and interacting online are all components of cybersecurity awareness [102]. Today, there is a clear gender gap in cyberspace. Many barriers hinder the advancement of women in cybersecurity. In addition, a lot of studies point out that IT (Information Technology) is a more male-oriented world, which is one of the reasons why so few women pursue a career in cybersecurity [77].

In a cyber security awareness survey in Bangladesh, a significant gender disparity is observed in choosing participants. With only 33.2% female compared to 66.8% of males [36]. Moreover, the survey focused only on undergraduates and postgraduate students. Consequently, under-representation of female participants overwhelms women's knowledge in cybersecurity and also results in women having less knowledge regarding cybersecurity. Concerning this limitation, our study will include different age groups of Bangladeshi women such as high school students, university students and working women. This allows us to cover more women's perspectives and the reason behind having less understanding of cybersecurity knowledge among women. Furthermore, several prior studies [108][81] highlight a significant disparity in cybersecurity knowledge between men and women. Their research found women awareness in cybersecurity is more vulnerable than man and found that women are more frequently targeted and affected by cyber-threats, where man victimization

rate in cybercrime is 35% less than women. This is indicating that women have considerably lower levels of cybersecurity awareness. Because of this knowledge gap women are more prone into cybercrimes and negatively impacts their experiences and safety in the digital domain [108][81]. Therefore, the key objective of this thesis is to investigate the reasons of women's having less cyber security knowledge, and to identify the main factor that is creating obstacles in acquiring better cyber knowledge. As well as, we seek to analyze for which situation and reasons women's behaviour negatively impacts cyber security. By understanding women's behaviour we discover potential risks that can arise. Lastly, this study implies effective suggetions and design a framework to mitigate the breach that is impacting the cyber security knowledge in our country.

1.1 Motivation

Cybersecurity awareness, knowledge and behaviour are essential components in mitigating cyber threats, as they influence the overall security posture of individuals and organizations [88].

With the increasing rate of internet users in Bangladesh, ensuring cyber security awareness is unavoidable. A huge population of Bangladesh has inadequate knowledge of cyber security practices. This insufficient awareness leaves the population vulnerable to cyber threats and attacks. A study shows, in term of cyber security practice, out of 802 participants 61% of total participants are always aware, 29% are sometimes aware and the rest of 10% are not aware of the legitimacy of the website they use. As well as, 77% of participants have been the victim of phishing mail and 71% encountered with identity theft [46]. Thus, people with high cyber awareness are more likely to be safe from ongoing cyber threats.

In [51], the author proposes strong correlation between users' personality traits and their intentions to engage in security behaviours. It validates that personality traits of agreeableness, conscientiousness, neuroticism, openness and extraversion will influence the user's security behaviour. As well as, it is discovered that the tendency of women getting associated with such risk has a big relation with sociological perspective and also the family structures. Again, the authors of [37] mentioned, the nurturement of patriarchal society views constructs emotional exploitation to the women of the family. The current transformation of joint family to nuclear family makes them feeling aloof, alone, bored and vulnerable. This eventually leads them to look for jobs or any other way to get through the loneliness accessing spoofy and harassing emails, websites or any groups. Furthermore, in [11] it is proven women tend to take more risk associated actions in career and social domains. It is also observed that risk taking behaviour tends to decrease with age so with that analysis, young women and girls tend to associate risks in their decision making. In recent view when it comes to working women, be it university going young entrepreneurs or any elderly, it is seen that nowadays most of the women are adapting with social media platforms to begin any startups. The president of BASIS, Bangladesh's largest association of software and information services, stated that around 300,000 people, about half of them women in the country are running their businesses with

the help of Facebook [69]. As they are getting directly involved in virtual business it is quite obvious for them to stay with different cyber risks, threats and bullying. Their lack of knowledge on handling security and information may result in further consequences.
A user may take an action which may appear harmless and end up bringing a dangerous interaction. As in, Facebook is despite all its device security a place where users easily can prey under scams [21]. The risks users tend to associate with email phishing, social engineered scams, personality traits and attitude has an impact on users being vulnerable in scams or cyberattacks [30]. As their attitude reflects on their concern about how their data is being handled. An observation from BBC in 2012 showed that hackers aimed at children's games and furthermore, according to Avast [100] it detected malware threats at more than 60 sites that contained "game" or "arcade" in their title. Children and youngsters are not particular about security when it comes to games. From this analysis it can be assumed that children and youngsters who play games via downloading it from third party websites have higher chances of malware infection. It is crucial to examine cybersecurity challenges faced by Bangladeshi women and the factors contributing to their digital vulnerability. To address these concerns, our study focuses on the following key aspects:

- After reviewing existing literature, we found there are many works that focussed on cyber security awareness but few research explicitly focus on women's cyber security awareness knowledge. Our study emphasizes especially on women of Bangladesh. Through our work we address women not only from urban but also the semi-rural and rural areas. By this process, the women of Bangladesh got highlighted, particularly their vulnerability to cyber threats.

- In the digital landscape of Bangladesh, high school students, university students & working women represent a significant portion of the digitally active population. Yet they are substantially facing critical cybersecurity risks and challenges. Therefore, this work seeks to determine cyber security awareness knowledge among Bangladeshi women.

- In the context of Bangladesh it is essential not only to investigate emerging cyber threats faced by women but also understanding the underlying factors that influence being digitally vulnerable.

- To establish a strong defense against cyber attack, amplifying women's voices is vital, thus to promote a safer and secure ecosystem, addressing women's perspective and choice holds immense significance.

1.2 Research Problem

Studying the current situation of Bangladesh regarding cyber infrastructure and law there is a need for cyber defense, security strategies and privacy policies in Bangladesh [63]. Women being crucial participants in digital platforms demands for a greater attention. But it is evident that women are under represented and vulnerable in the cyber realm. Individuals personality traits and peer influence significantly impacts their ability to ensure a safer digital environment.

Based on the in-depth analysis of existing studies, the following research problems have been identified to address the cybersecurity awareness challenges faced by women in Bangladesh:

- A large demographic of women are more prone to getting victim of cyber attacks. It is important to highlight that there is a vulnerable state of cyber security awareness knowledge in Bangladeshi women.
- Lack of insufficient resources and cyber education in rural and semi-rural areas hampers to obtain fundamental cyber security awareness knowledge and leaves them into a unprotected condition to the digital space.
- Additionally, women's personality trait and situational state influence them to associate with the risks and vulnerabilities.
- Finally, the cyber defense framework of Bangladesh is not properly constructed for women. Thus, implementing proper design and strategy is crucial.

1.3 Research Questions

The research aims to investigate and try to answer the following research questions:

- **RQ 1:** What is the current state of cyber security awareness knowledge among Bangladeshi women?
- **RQ 2:** What are the potential risks and threats faced by women due to their cyber security awareness level?
- **RQ 3:** What human behaviour and situational factors influence women to engage in risky cyber decisions?
- **RQ 4:** Which design interventions can be proposed to enhance the cybersecurity system and overcome the knowledge disparities among Bangladeshi women?

Expanding on these questions, we aim to evaluate the awareness level of cyber security of the women of Bangladesh and the possible risk and threat that can be associated human behaviour.

1.4 Research Objectives

The research objectives are established to provide a thorough insight of cybersecurity awareness level and the correlating aspects that are related to cybersecurity awareness. By identifying the possible arising threats and gaps, we aim to provide a complete solution to our obtained findings. The key objectives for this research are as follows:

- **Objective 1:** To assess the cybersecurity awareness level among different women groups of Bangladesh.

  - Analyzing cybersecurity awareness by focusing on women's knowledge, practice and security measure.

- **Objective 2:** To analyse the risk and vulnerability arise from women's inadvertent behaviour.

  - Identifying the consequence that arrives from women's online interaction and activities, substantially cyber-threats.

- **Objective 3:** To explore the background reasons that influence individual's attitudes and behaviours towards cyber threats and security measures.

  - Unveiling human behaviour and situational factors that influence women into cyber risk.
  - Assessing women's response to security warnings.
  - Understanding women's action and inaction to their experienced cyber threats.

- **Objective 4:** Through examining the overall finding, we seek to propose an effective solution and make a design intervention that would safeguard the ongoing cyber security system along with overcoming the cybersecurity knowledge disparities among the women of Bangladesh.

  - Identifying women's perspective on security and privacy features.
  - Exploring women's provided insights for enhancing cybersecurity awareness.

Through achieving the outlined objectives, this research contributes to the broader goal of improving cybersecurity awareness and resilience, providing valuable insights that can inform policy-making, educational initiatives and targeted interventions to safeguard women against evolving cyber threats.

1.5 Contribution

Numerous existing work explored cybersecurity awareness, but limited research focused particularly on women's cybersecurity knowledge. Especially no existing work that covers diverse age groups of women across different areas of Bangladesh. Ranging from urban to semi-urban and rural our work addresses women inclusion profoundly. Examining through a large scale survey and in depth semi-structured interviews, this work evaluates the cybersecurity awareness knowledge among Bangladeshi women. Our work comprehensively uncovers rapidly emerging cybersecurity threats faced by women. Our findings reinforce that women being victim of cyber attack is driven by lack of knowledge along with behavioural tendency and situational factors. We studied women's understanding of security warnings and their approach to handling cyber threats. We identified potential barriers that prevent women from confronting their cyber security related threat. Additionally, we explore women's insight into security, privacy and digital policies throughout their digital interactive. Furthermore, the proposed framework can assist women from diverse backgrounds

to overcome their knowledge disparities. Our work can enlighten other research to emphasize more on the driving force behind the women. This work contributes to HCI community by addressing women's cybersecurity awareness knowledge, digital challenges, technology barriers, behavioural and situational factors to bridge the gaps and foster safer digital space.

1.6 Thesis Outline

Our thesis will follow a chapter-wise organization as given below in Figure 1.1.

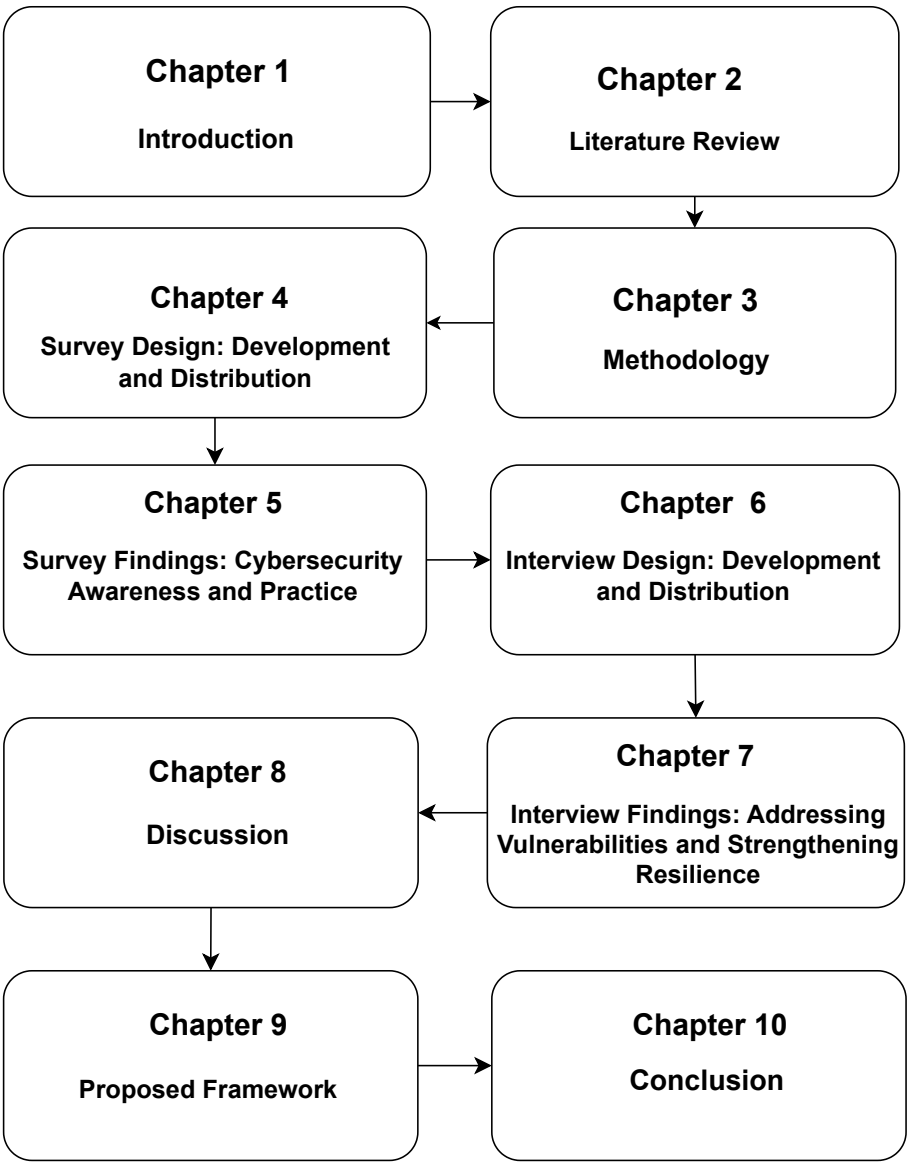

Figure 1.1: Thesis outline

Chapter 2

Literature Review

This chapter will provide a rigorous reasons of why Cyber-Security Awareness (CSA) should be incorporated into women's everyday lives. There are two following sections that will also examine the impact of CSA. We generalized them as cybersecurity knowledge in Bangladesh and global awareness of cybersecurity which is basically showing the CSA situation in two different perspectives. It also included the potential liabilities that a person or an organization may face for their failure to maintain cyber security or to notify the public when an attack on information occurs.

2.1 Cybersecurity Awareness in Bangladesh

In [107], the authors proposed the factors that are influencing the adoption of information security awareness. Developing a measurement model they proposed six hypotheses. Complementing with the hypothesis their result provides that device password, social network safety and cyber law has a significant impact on security awareness adoption. In contrast, use of antivirus software and firewall has an insignificant impact on the adoption of information security awareness. However, they did not explore the root cause of this.

In the evolving digital landscape, the authors in [96] investigate the critical role of cyber security awareness among university students. Keeping cyber security as a mediator it focused on cyber security knowledge, password security and self perception skill. The authors surveyed 430 students and analyzed that students with higher levels of cybersecurity knowledge are more aware of developing strong cybersecurity habits. It is observed that having good practice in password security also significantly enhances cybersecurity awareness. The research emphasizes cultivating cybersecurity awareness for being prepared to engage oneself in the digital world of industry Although, this study does not provide concrete strategies to implement for effective awareness knowledge. Delving deeper into cyber security challenges coming from industrial sites could assist more knowledge.

In[46], the author aims to secure the digital environment of Bangladesh by identifying different demographic groups and developing strategies. Exploring factors like age, education level, gender and location an individual's personal understanding in cyber security practice and awareness may vary. Analyzing a connection between cyber security knowledge and educational background more effective awareness cam-

paigns can be designed. As currently in Bangladesh there is only one-size-fits-all approach for cyber security education, the author refers to the importance of understanding demographic variation to identify the knowledge gap. Once the gaps are identified educator and policymaker can design targeted and appropriate educational programs considering each demographic specific needs. On the basis of these findings, the author draws inspiration from Europe, US and Japan then describes the approach of awareness strategies. Recommending governmental initiatives, media involvement and educational integration in the system. Finally, this paper aims to enhance the cyber security awareness in Bangladesh.

Ferdous et al.[105] basically conducted a survey consisting of questions regarding the level of awareness our GenZ have which includes their demographic information, cyber knowledge, cybersecurity activities, and cybercrime Consciousness. The aim of the paper is to construct a solid cyber security framework for Bangladesh, an in-depth analysis of what GenZ knows about cyber related crime, security measures and ways to avoid threats. Following a mixed-method approach that mainly contains- 1. extensive literature review for secondary data and 2. quantitative survey questionnaire (17 MCQ) to collect primary data the publishers targeted the audience of GenZ, belonging to the BBA curriculum of both private and public university students using convenient sampling techniques (frequent and easily accessible individuals). The limitations of this paper that have already been mentioned by them are that just depending on only 545 participants they made the survey which does not even hold 40% of the target audience [105]. The paper has not delved any further and does not offer suggestions on how to pratice and develop cybersecurity awareness.

To assess the impact of human factors on cybersecurity, the author in [94] highlights employees behavior in safeguarding organizational security. Difference in employees cyber practice emphasis in having personalized training programs. Using unauthorized software makes the system vulnerable to malware attack. Their analysis shows malware encounter rate during the third and fourth quarter of 2015 in Bangladesh, where unwanted software like browser modifiers affects 15.6% and software bundlers 13.7% of all computers [94]. Endpoint security and data protection technique is emphasized as a crucial component for preventing cyber threats. Cultivating a cybersecurity-conscious and implementing leadership practice in an organization is highlighted as a key factor in shaping secure cybersecurity practices. Beside this, ensuring licensed software for employees has a crucial importance in data protection.

In [86], the author discussed how through social engineering attacks the internet users of Bangladesh are facing cyber crime. Due to the lack of education on online privacy and security the rate of social engineering attack is increasing day by day. Moreover, the study found the security system of E-Banking is at risk. Most of the employees use weak and easily identifiable passwords which is making them an easy target of cyber attack. It is observed that 50% of participants in a survey use the last 6 digits of a phone number as their password [86]. This action indicates the vulnerability of password security. However this research is limited by the few questions about password security and did not explore more on password security complexity and other areas of security features.

Uddin, et al [108] discussed the cyber security awareness challenges in Bangladesh. Identifying the factors contributing to cyber crime in Bangladesh it shows how different challenges pose. Password sharing habits and using a common password are one of the highlighted factors. Users often tend to share their personal information to strangers unknowingly. It is also observed that some users often share their location on social media. Associating with installing malware instead of authentic software is a significant concern. The relationship between cyber security is also examined, finding women experiencing more cyber crime than men. Mentioning potential solutions like imposing government initiative for cyber training, regulating data backup, discouraging download from unreliable sources and being cautious in sharing personal information, this study measures essentials to enhance cybersecurity awareness and security protection in Bangladesh.

Cybersecurity of a country depends heavily on organization structure and its members being cyber conscious to keep themselves updated against ever-evolving cyber threats while abiding implementation of cyber laws in cases of cyber-abuse. According to [95], personal data of over fifty million Bangladeshi citizens was extracted and exposed from the Birth and Death Registration (BDRIS) website of the Office of the Registrar General and was found in Telegram. The compromised data included the full names, phone numbers, email addresses, and national ID numbers of the affected individuals and could be easily accessed in Telegram if NID number and phone number were given; endangering many people to identify theft and social engineered scams. Furthermore, it is observed that, despite BDRIS being identified as the source of the data breach, no actions have been recommended or taken against them by the investigating body. The ICT division acknowledged the problem but did not enforce cyber security laws upon the culprits which encourages perpetrators to commit these sort of privacy violations and remain uncharged and without consequences.

An old incident of Bangladesh cyber attack $81M Bangladesh Bank heist backpedals to 2016 when digital security of a government bank "Bangladesh Bank" was easily infiltrated by an employee who had accessed a malware laced email, causing an international scandal as well as a goose chase for $66.4 million dollars which remains undiscovered till date [65]. This incident had showcased the lack of malware detection and awareness. Unfortunately, it is still observed in [101], that malware attacks are still prevalent and recently have caused serious privacy infringement, data loss and business forfeiture throughout Bangladesh.

[35] attempts to make the readers be introduced to potential threats that occur in a country in response to the globalized view and exacerbates the cyber security of Bangladesh. In this internet centric world the threat and associated risks of cyber is not a national issue anymore rather a global concern which Bangladesh lacks in many aspects. With a view of political proprieties and a digitalized vision the country is actively participating in the cyber world yet getting targeted in different cyber crimes through a form of traditional criminal activities. Along with a vast use of pirated software the authors categorized other cyber crimes into four different sections - crime against individuals, property, organizations and society. To summarize these

concerns there are some mentioned policy remedies like reforming legal structure, maintaining rules and regulations and spreading awareness with vivid explication.

2.2 Global Awareness of Cybersecurity

In [98], the authors highlight the disparity between men and women's participation in the cybersecurity workforce. The author emphasizes on how systematic bias in the recruitment process, work culture environment and support impacts on women's participation in cybersecurity roles in the workplace. It is also stated that though numbers of STEM graduates are increasing but the gap remains undisclosed due to lack of support and guidance. It proposes a few suggested solutions on how this problem can be lessened but the effectiveness of the proposed solutions are not stated.

Further supported by [20], where the authors underscores on some factors such as social influence and personal challenges in the career field which resulted in women being under represented in the cybersecurity community. The authors conducted interviews and paper surveys to collect data to analyze them. Upon inspection, few issues were acting as prominent barriers to career advancement such as lack of implementation based knowledge, insufficient guidance and inadequate team support.

In [19], the author investigated his general views on how women are getting victimized through Social Network Websites (SNWs) along with his perception of such victimization coming from socio-legal-victimological angle. This analysis comes up with the causes of such victimization in a widening scale relating to our objective as well. Karuppannan mentioned in his research that the pattern of women being victimized can be of different types (victim's sexuality, ideologies, professional commitments etc.) by which following them the offenses are too many to get through. Along with some basics like hacking and harassment, he found cyber defamation, cyber stalking, Morphing sort of crimes. In [19], mostly emphasized on the virtual threats women are facing in SNWs. Based on our motive this research has not conducted any reason behind having these troubles and how we can come up with some steps to avoid those.

In [70], the authors explore how personality traits and self-reported knowledge can predict risky cybersecurity behaviors. It shows personality traits such as conscientiousness, sensation-seeking and knowledge about passwords influence the cybersecurity behavior. According to their findings, conscientiousness is linked to lower cybersecurity risks for women and sensation-seeking is linked to higher risks. Their result indicates that general risk-taking behavior integrates to higher cyber security risks. For example a person high in sensation seeking potentially susceptible to clicking on suspicious links. Their findings highlight the potential for using personality assessments to improve cybersecurity awareness.

Highlighting a complete picture of the cyber awareness and concern level of adult women of rural Punjab, the author emphasized on the defenses to adopt for this particular demographic sector. In [103], the initial web-based survey has been con-

ducted on different demographic sectors which further led the author to concentrate on younger people who seem to be more vulnerable and at high risk compared to others. Even though targeting a specific audience researchers analysed the survey data with a broader sense of different demographics. Later on, based on the findings this research came up with necessary recommendations to follow like realistic training, cyber security prototype which is basically a decision tree of series of questions to make an appropriate decision. The author successfully managed to show us the awareness level of different demographic sectors in rural areas of Punjab regardless of any fixed motto to focus on. From our review we comprehended that it will analyze young adults but given the data analysis it brings up the whole community eventually coming up with solutions only for the people aged between 18-29 years old.

In [53], a survey was conducted targeting the audience of second year university students where the authors took the help of cyber security of Malaysia for a 3 hours interview of the victims to share their stories of cyber threats. Based on their research it is found that the students demonstrated a good qualification over their awareness level on different cyber fields although it is also seen that the failings are still there in cyber-harassment and how to protect themselves from falling for the traps of those. Computing the cumulative means of different constructs of their study it is quite apparent that only for cyber-sex (3.99) and self-protection (2.89) the variable is less than the others. Even though the whole research focuses only on measuring the variety of threats these students can face but concludes with a short note on emphasizing the importance of education in every phase of student life for the increase of cyber awareness level.

In [71] it investigated the stages of understanding cyber security awareness among secondary school students along with their teachers and parents. To fetch the necessary data the authors deployed both online and offline questionnaire surveys categorizing for each of the population. With further investigation the authors show the importance of education in developing cybersecurity acknowledgement as early as in secondary schools. To begin with their findings they prepared the close-ended questions for each of the three demographic categories to identify the current level of awareness which led them to their second phase of distributing the questions to the audiences. The authors themselves collected 98 samples of students and consecutively from teachers and parents to access the larger sample size. The final phase of their study involved data analysis, findings and recommendations. In the findings Zulkifli et al. mentioned that students may be aware of personal data but less exposure to the impact of online activities. Additionally, parents and teachers may be aware of the threats but lack of practice brings up the insecurities to face both at home and school respectively. The contradictory part of this paper is this whole study was conducted limiting to a specific region, therefore whatever the result the publishers came up with can not be said to be entirely applicable for all cases rather it can vary. Also, it could not be maintained that in a paper-based method all questions are getting answered as it is highly essential to get the fitting findings.

Carroll [6] focuses attention on the evolution of HCI and design and software principles while focusing on human's social and behavioral science for improvement.

Initially till to mid 1970 HCI research papers were not focused on users and usability according to the author. From 1990 onwards, ever since HCI began to incorporate itself into computer science, it began to bring new prospects of studies outlining user needs and interactions for project planning and understanding design rationale. Hence methodologies on usability evaluation began to develop systematic approaches to ensure cost effectiveness (Bias & Mayhew, 1994). HCI continues to influence and evolve to the date hence it is implied there is no fixed solution to any problem and for any solution, user feedback and cooperation is crucial.

It is undeniable the role the user plays on security failures and system designers must address those user behaviors to build more usable and efficient systems [9]. Furthermore, the authors underscores some user stories to highlight how some systems may inadvertently set users up for failures as many user issues with security mechanisms arise because they don't align well with users' goals and tasks. Users primarily act based on their objectives, any obstacles that impede it are not viewed favorably by the user. Sasse et al. [9] implies system design should vary according to its usage to uphold its security while enforcing organizational structure on cyber security practice and upholding its practice in accordance with cyberlaw while understanding user's behavior to prevent user mishaps with stern hand. Furthermore, the authors draw connections between password, password policies, varying systems and user memorability issues. One key HCI principle is to reduce unaided recall, as it increases cognitive load and hampers user performance. Hence a study was conducted with types of passwords and system based visual authentication. Although system based visual authentication yielded good results but as users were cued and study was not completely unmoderated. When there were multiple uses, it gave rise to the same sort of problem users had with passwords.

This investigation reviews the cyber security awareness knowledge and the after effects of cyber attacks, conducted through a Q/A session among the students of Kyrgyz-Turkish Manas University. The questions were formed focusing on the factors of malicious software, password security and social media security. After going through extended reviews of the papers of different methods and approaches. The researchers claimed their findings to be different from other papers as it carried out the part of the online education process. The manifestation of five different relations has been made in [84] at the beginning phase. Relation between cybersecurity knowledge with demographic factors of students gender, age, major and education level has been conveyed following the effect of the method of internet connection on awareness. Further association-ship has shown relating to cyber attacks resulting in the rate of those who have encountered a situation such as having their password stolen or their account hacked in an online system is 23.0% and double of the rate of them who have not heard the terms of "Social Engineering" and "Phishing Attacks" of who have heard [84]. It has put stress into education on cyber awareness as the study evaluated the survey was more competent for the students who have it. It is mentioned that researchers pointed out to make the survey more qualitative via other methods like in-person interviews or evaluation exams to increase its coherence.

The level of cyber security threats, the experience of incidents and the likeliness of experiencing them in future-all confined in the survey data of the students of a

western university of US belonging from all levels. The authors make the readers recognize core concepts of understanding cybersecurity from students' perspective revealing the gaps in them. As per [41], it focuses on the importance of cybersecurity education in the university framework and urges teachers to use innovative methods and to be informed about the latest developments in cybersecurity. Future research should also aim at comparing the level of knowledge on cybersecurity among different cultures besides longitudinal research to establish the pattern of the development of perceptions towards cybersecurity.

Aiming at the relationship between cybersecurity awareness and practice this paper depicts the significant impact of cybersecurity. The future holds on the next generation, hence targeting them with the advancement of technology, Muhirwe et al.[45] developed the survey questions based on the NIST 800-50 publication and following some recent studies. A five point likert scale was used to perceive CSA and knowledge of the targeting population. Using a web-based survey service provider, qualtrics, the survey got distributed via mail including all necessary information. The structural model assessment pictured a calculative analysis on different paths of training and event respectively to awareness path and finally reaching to practice alongside different demographics. To summarize their findings they managed to establish the proof that practice brings up good accuracy, while only awareness did not. The mentioned limitation part is to conduct a qualitative study through interviewing the ones who attended the events of cybersecurity, the reason behind joining and analyzing how it helped them in the long run.

In [34], the authors highlight the extensive need for cyber security awareness due to the growing dependency on the internet in South Africa. It proposes a government-led, multi-layered framework to address the knowledge gap. The framework involves creating a national vision, suggesting specific programs, developing educational content, identifying target audiences and monitoring progress. The action plan emphasizes the ongoing development mostly through analysis and modification.

Al Kandy, S. [97] has highlighted the challenges of implementation of cyberlaw in the digital landscape in developing countries such as Indonesia, Kenya and Brazil. It is implied that resources of developed countries fail to provide for the challenges faced by developing countries. The disparity of information highlights the need for more region-specific analyses considering these countries' socio-economic, cultural and political nuances. This research follows a normative approach to examine the evolution of cyber law governance in the following countries and underscores the importance to harmonize cyber laws with fundamental rights, including data privacy, freedom of expression and access to information, while also ensuring regulatory adaptability to keep pace with technological progress. Moreover, it emphasizes the significance of lack of resources and technical expertise that affects the implementation of cybersecurity measures and how lack of coordination amongst government bodies, private sector entities and civil society contribute to inconsistent enforcement practices.

Rakha, N. A. [92] examines the laws that regulate cyberspace in Uzbekistan, with issues like privacy, cybercrime, data protection and intellectual property rights. The

author uses a doctrinal research approach to analyze the legal structure of cyberspace as well as its effectiveness in safeguarding it. The research findings by the author underscore the importance of understanding cyber law awareness and its implementation, enhance investigative ability and secure international cooperation to secure its digital space. Although Uzbekistan is successful in its application of legislative measures in areas such as data protection, cybercrime, privacy and intellectual property rights, showcasing its commitment to addressing the challenges of the digital age. Cyber threats are constantly evolving therefore, there is a need for cyber justification to evolve as well.

The study by Hong et al. [90] delved into the intricate relationships between work overload, job stress, corporate ethics and cybersecurity behavior among employees in South Korea. By using various measures and data analysis techniques, the research aimed to uncover how work-related factors influence cybersecurity practices in organizations. The research findings revealed that work overload can indirectly impact cybersecurity behavior through job stress, with corporate ethics playing a moderating role in mitigating the negative effects of work overload on stress levels. These insights provide valuable theoretical and practical implications for organizations to manage workload, stress and ethical climate to bolster cybersecurity measures. The researchers surveyed 377 employed people in South Korea over three time points. They used online surveys to collect data on work overload, job stress, ethics and cybersecurity behavior. They analyzed the data using correlation analysis, factor analysis, and structural equation modeling. The study followed a strict process to ensure the accuracy and reliability of the results. The sample size was determined by considering various recommendations from prior research. Overall, the study sheds light on the importance of considering human-centric factors in cybersecurity strategies to enhance organizational resilience in the digital age.

Grobler et al. [76] displays the expansion of the improvement and constructed a human centric domain of cyber security. The three prime components of cyber security user, usage and usability. The author traverse the rapid growth complexity of cyber security and focuses on transformation in model from functional to usage center. This work provides the foundation for incorporating the entirety of humans into cybersecurity system architecture design. It focuses on the idea of the invisibility of security and esotericating particular tasks while maintaining people's engagement and using the intelligence of machines. As a result of this symmetrical human-technology interaction, the review highlights three distinctive features to advance the cybersecurity field.

In [74], the author discusses phony phishing management techniques (ActionCode, education and training CourseCraft) as other layers that have specific benefits, circular enough to cover the circulation in its area model. Phishing is a significant threat and as such we will almost certainly continue to implement these extensive strategies in the future to protect our users. They require legislative and enforcement measures, though legislation is not practical due to the fleeting time frame of attacks as well as jurisdictional matters. While user education/training have their place, as well as visual cues to increase awareness and lessens vulnerability, some users will balk or ignore the training. Blacklists are only effective if the phishing

detection is accurate and updated, giving help on what online communities do to share information around detected phishing incidents.

Again, In [7], the author conducted an empirical study on the computer users at the Department of Defence installation in California. The main objective of the study was to analyze the characteristics of users' selected passwords. Examining the relationship between passwords, it found the frequency of the password used depends on the user's necessity of inventing new passwords to access data. Without sufficient need to change or update passwords, it remains unchanged and at higher vulnerability if the said password is used at multiple sites. Highlighting the relationship between password complexity and memorability, it is found frequent change of password and password selection method were responsible for difficulty in remembering passwords. In the aim of securing information security this research provides critical insight of password security. By an empirical evaluation of password practice it reveals common flaws in user password practice. After all, password security reflects individual understanding of safe practice.

Employing a qualitative approach to analyze the privacy concern of South Asian women, In [56], the authors provide an in-depth analysis of how women perceived, managed and controlled their privacy while sharing devices. Examining 199 female participants from India, Pakistan and Bangladesh this study shows that women's privacy gets violated deliberately or unintentionally because of device sharing. Monitoring women's devices by their social relation has become a very common practice. Also, due to cultural norms and having less technical knowledge women herself often share their personal mobile phone with their family members. Some women find this device sharing practice helpful to them while some groups feel insecure. Moreover, this study also provides different privacy practices imposed by women to maintain some level of privacy on their device. Such as, app locks, entity deletetions, private modes but unfortunately often this method fails because of some social restrictions. Finally, for better support in the privacy of shared devices this study suggests understanding the cultural norms and value of the women first . By this, an improved design can be built to educate and aware them in protecting their privacy effectively.

In [36], the author explored employee awareness of cyber security and made a HAISQ (Human Aspects of Information Security Questionnaire) model by validity testing, pilot study and main study to examine the relationship between policy, behavior and attitude towards using a work computer. This model includes several focus areas such as, email use, mobile computing, information handling and analyzing user knowledge, attitude and behavior. Strengthening employees knowledge in information security progressively impacts on their attitude and behaviors. To improve organizational security training programs, identifying the link between employees' knowledge and attitude is important. This research aims to use this HAISQ tool to have a detailed assessment over employees' information security. Using this HAISQ model organization can ensure their employees better security awareness knowledge and also can mitigate possible security risk.

In [61], the authors investigated cyber security awareness in students of higher education in India. They researched some categories such as based on gender, residential

location, nature of the courses, students levels of study, academic discipline level of study and built questionnaires for the students to participate in. The authors analyzed the survey by statistical tools. Their findings show that semi urban students are more aware than the rural students. Moreover, students who are in professional courses are more likely to be aware than the students who are in general courses. In addition, students who are in post graduation are more aware of cyber security compared to the undergraduates. On the basis of discipline the students of science are more aware of cyber security than those in other disciplines. The research is limited as the survey they conducted was from the same institution. Moreover, there is still a scope of considering how part-time jobs of a student might influence cyber security knowledge.

In [93], the authors argue that cybersecurity as a dynamic subject would benefit from different perspectives and show how principles from world religions can inform cybersecurity especially in the context of ethical, social, and behavioural issues. As over the last decade we have focused on trying to secure personal computers and devices, this argument has prompted a reconsideration of old school cybersecurity for which one of the loudest wake-up calls was an indication in this same month that cyber-criminals had attacked the software was that managed some U.S. government computers using a legitimate password, rather than a vulnerability in the software itself. From both cybersecurity and an ethical perspective, religious ethics offer great guidance. Jewish ethical monotheism and Buddhist righteous behavior, for instance, exhort people to follow good cybersecurity policies and to behave better online.

Cybersecurity as a religion favors community and the community commonwealth of resources. The Islamic concept of Ummah and Christian communal solidarity argue for fostering a culture of mutual vigilance and collaboration inside organizations [93]. As per author, religious rituals can function as a trigger for establishing consistent cybersecurity habits. Islamic prayer hours and the Jewish Sabbath encourage intense, ongoing security drills and updates. Religious storytelling effectively conveys moral teachings. Storytelling may help with cybersecurity training by making the consequences of breaches and the importance of vigilance more personal and memorable. Integrating concepts from other religions results in a more complete approach to cybersecurity. Ethical lectures, community support, ritualistic discipline and engaging stories can all help to enforce security practices and foster a good cybersecurity culture.

According to Daengsi et al. [83], cybersecurity awareness is critical when it comes to mitigating risks associated with cyber threats, especially phishing attacks. The authors seek to highlight specific age and gender-related consequences of staff cybersecurity practices that have typically been overlooked, particularly in the case of Thailand. In paper [83], their research was mainly based on 20,000 employees of a major financial company on the nationwide level in Thailand. Staff cybersecurity awareness went sky-high, and as a result, the number of phishing emails dropped with 71.5% based on the numbers found in the study [83]. The difference in cybersecurity knowledge emerged only by gender, where female employees were more knowledgeable than males, while a varied generation from Thai employees did not

affect cybersecurity knowledge. The survey was designed to measure security awareness and attitudes in general and took a closer look on age and gender, by means of a questionnaire on the understanding, beliefs and behaviors related to their personal information security and the knowledge of phishing attacks. It also performed a statistical analysis to reveal trends and relationships between demographic parameters and cybersecurity awareness, comparing average scores over age brackets and gender. There were age and gender differences where the oldest employees knew best and men are only marginally better than the women. This suggests that tailored training programs that cater for preferences of certain cohorts in combination with ongoing monitoring and adaptation to keep pace with evolving threats are necessary.

People are showing less interest in the traditional form of learning and getting aware of cyber security which is why Huynh et al. [48] came up with the concept of a game to make the users acknowledge the concept. Activity Theory-based Model of Serious Games (ATMSG), a developed model as a training tool to create a scope for the end users to comprehend cyber security awareness while playing games. The structure of this method is quite coherent and reprehensible as this will be based on "Story Gameplay" where players will experience different scenarios and events. Focusing on those situations participants will show their activity through solving and practice. To investigate the productivity of their design they conducted a short survey where it resulted positive for the beginners but seemed the interest level is higher for the intermediaries. The reason behind it becoming less captivating for the beginners as the makers used new terms and materials making it less enjoyable to them to access.

2.3 Our Plan

Our literature review has thoroughly examined the existing work within our research area. Evaluating the cyber security awareness level, most of the studies did not go through the detailed examination on women. There remains a significant gap in understanding underlying factors that are associated with women. Therefore our research aim to focus on women's cyber security awareness knowledge and aspires to investigate in depth into the underlying reasons behind the women's as a victim of cyber threats. Analysing through human behaviour and situational factor that influence women to associate with risk and threats, this thesis aim to address women's perspective, response and their needs. To effectively address the issue, our research has proposed vigorous suggestions and proposed a design intervention that will strengthen the current cybersecurity awareness and cybersecurity system in Bangladesh.

Chapter 3

Methodology

The usage of digital technology in everyday life has grown rapidly, enabling people to work from home remotely, manage daily tasks, and stay connected with others more easily. However, with these technologies there come vulnerabilities and women, specifically in Bangladesh, are still largely under represented in cyber security. Our research aims to pinpoint the state of cybersecurity knowledge among Bangladeshi women: high school students, university students, and working women who are now engaging in different digital platforms. For our study, we have done quantitative and qualitative data collection on three different groups of the female population. In phase 1, we proceeded with a survey to measure their understanding regard to some general topics of cybersecurity such as Password Security, Information Security, Device Privacy, Incident reporting, and Malware detection. This is all to analyze if any correlation could be gleaned from the data regarding these factors. Which analyse the current state of cyber security knowledge among them. In phase 2, we did qualitative data collection via semi-structure interviews. Through semi-structured interviews, we analyzed the participant's experience, behavior and practice in the cyber landscape. Finally, we acquired participant's preferences and their needs, to bridge the gaps. By these approaches, this study delves into their understanding, behaviour and risks that is influencing in their cyber domain. We finally examine these and provide a relative simulation and solutions towards enhancing cyber security consciousness among women in Bangladesh.

3.1 Hypothesis Development

Traditional text-based passwords remain the most widespread form of user identification. Hence, services attempt to safeguard their clients by providing improved and safer, technologies for identification authentication. According to [42] in their study, it has been stated that they have looked over 1,11,000 users accounts if they have enabled the two-factor authentication (2FA) for their two step verification. Out of all those accounts 6.39% of them use 2FA. It has become very clear that users have a very difficult time trying to deal with multiple passwords that they are trying to remember [14][13]. Today, it is standard that the user chooses a few strong passwords and reuses them across different services [15]. Changing or recycling passwords can be dangerous if a leak happens in doing that time [14][23]. As a result, web services have had to incorporate server side measures being deployed to curb password hacking. Among them, the most popular and well-known is two-factor

authentication (2FA). In our study, we are looking for the same issues happening for the women of Bangladesh, in the terms of reusing passwords and trying not to use 2FA continuously or consistently. This was to test our hypothesis regarding whether always or mostly linkers are less likely to turn on 2FA than rare or never linkers. Therefore, we developed the following hypothesis:

H1: Women who reuse passwords across accounts might be less likely to consistently use 2FA.

Social media platforms serve as a network mediated world that are analogous to some face-to-face activities of everyday life. They allow interaction with a broader number of people (as characters in the world could potentially be millions of users) and can be accessed at any time of the day as they are available around the clock in contrast to [66]. However, as it is mentioned in [55] that all of the approaches have the negative impact of cyber bullying and there are very severe cases, but none of the approaches do not allow the corresponding misbehavior and solve the problem fully and efficiently. As the trend of cyber bullying is rapidly growing, these techniques have been proved to be inefficient. Help-seeking is considered as the "activity which implies seeking of assistance from other individuals" [12]. It is viewed as a constructive way of dealing with stress which is beneficial at any stage of the life cycle and enables the reduction of painful psychological signs. Although in the literature, it is recommended for a victim to report a cyberbully since it helps in stopping the situation, there have been studies suggesting that students are reluctant to report cases to a helpful adult such a teacher or a counselor [28]. In fact, children and adolescent cyber victims are even less likely to seek help and report the bullying to an adult in contrast to the traditional bullying victims [16]. The findings in [43] of the present study revealed that the perception that reporting cyberbullying would lead to it's stoppage was the primary reason for the enhanced intentions to report cyberbullying. To establish a culture of reporting, the individuals responsible for the task must ensure that a cyber victim's report is well dealt with within the shortest time possible. In our research, we assume that cyber bullying somewhat makes people more aware about the cyber attacks. Thus we come to the following hypothesis.

H2: The confidence in women's ability to handle cyber-attacks correlates with reporting cyberbullying incidents.

Studies have found that age and gender are independent variables of susceptibility to phishing conflict with overly generalized assumptions. The studies regarding age facts stated that age did not predict risk or susceptibility, whereas some other articles indicated that young people are more susceptible whereas two are more susceptible than older people. Depending on the statistical procedures, 'younger' and 'elder' were defined differently, although the majority of the studies analyzed correlations or regression coefficients and a few used ANOVA test for between-group comparisons [22], [24], [26], [60]. Likewise, gender analysis revealed that 24 out of 35 studies found no significant difference in their performance on detecting phishing attacks though 9 studies revealed that females were more susceptible to phishing while only one study showed that male participants were more susceptible to the attack. These are conflicting studies and a meta-synthesis is required to determine

the relationship between age and gender in phishing susceptibility [31]. So for our study, we develop the following hypothesis :

H3: Women's field of study and employment correlates with their ability to identify phishing examples and malware detection on their device.

To demonstrate the complete plan of our study, the following methodology workflow diagram is presented in Figure 3.1.

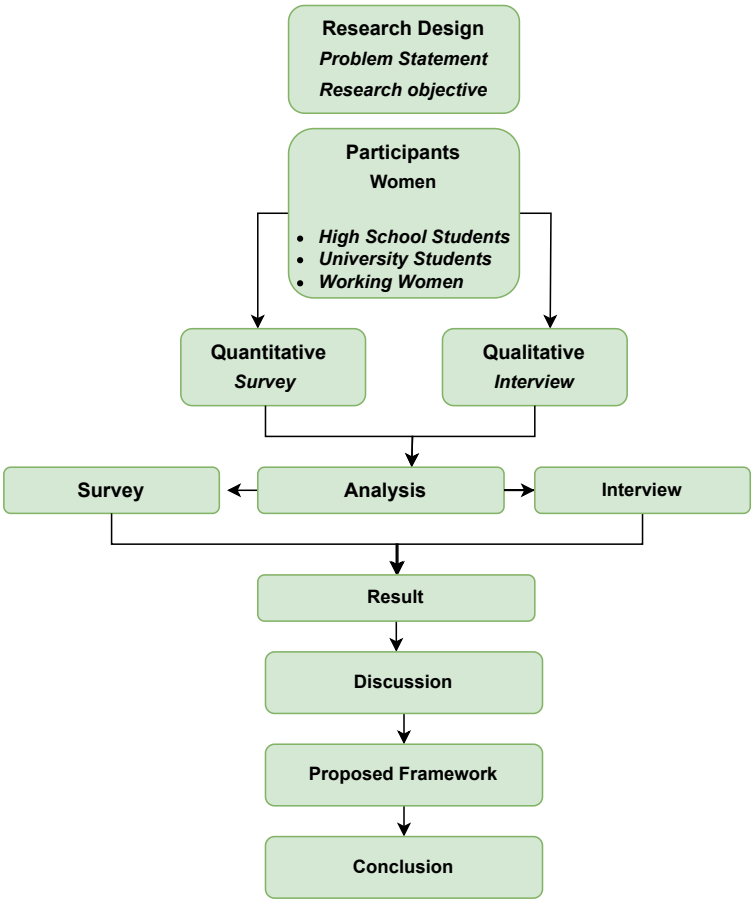

Figure 3.1: Methodology workflow

The Methodology workflow in Figure 3.1 defines the overall process this research has been followed. A step by step breakdown of the whole study is portrayed here.

3.2 Participants

Reviewing through many distinguished papers in both global and Bangladesh perspectives, we found research specifically addressing women's challenges in cyber security remains unaddressed. Recognizing this gap, we chose the women to be our main focus of our study. To have a greater exploration, we categorized them to subgroups such as: high school students. As high school students are vital in shaping digital space and formatting their digital habits from a very early stage. They have some general notion of cyber security but are devoid of self protection awareness which makes them become more prone to cyber threats. after that we chose university students, the high rate users of the cyber world depend from time to time for frequent use. This group has an increased autonomy and exposure. The number of women working in the literate sector is still under-represented in Bangladesh. Yet their roles in some important sectors, ask for a better cyber security knowledge. Thus, understanding working women's cyber security knowledge and practice is essential. To get an in-depth analysis we choose quantitative & qualitative methods. For quantitative method we performed survey where there are (n=1,202) participants. For qualitative analysis we performed a semi-structured interview with (n=30) participants. Coming from the view of Bangladesh being such a population country raises a question if the women of this country are knowledgeable enough to deal with the emerging cyber threats or not. And if not, why, the prospect of the question led us eager to choose them as our target audience.

3.3 Data collection for Survey

This section give an overview of survey data collection process for assessing cybersecurity awareness among Bangladeshi women. Starting from survey participant, survey conduction, selection of sample size and data pre-processing for survey.

3.3.1 Survey Participants

Our study is based on the awareness and knowledge of Bangladeshi women and their cyber behavior in the cyber world. We have chosen three different demographics for the detailed observation of our study and they are high school students, university going students and working women. Table 3.1 shows the demography by group and age range of all participants

High school students: In our survey, the sample size of high school students who participated in the survey is 761. The age range for the high school students is from 12-23 years. By this manner, we have gathered their point of view of privacy and security practice.

University students: We also conducted a survey for the university students and the sample size is 333. The age range is from 20-31 years. From the collected data, we were able to analyze the different perspectives of them.

Working Women: Lastly for our survey, the sample size of the working women is 108. The age range is from 20 to 43 years and above.

Group	Number of Participants	Percentage (%)	Age Range
High School Students	761	63.31	12-23
University Students	333	27.70	20-31
Working Women	108	8.99	$20- \leq 43$
Total	1202		

Table 3.1: Demographics of survey participants by group and age range

3.3.2 Survey Conduction

A total of (n=1,202) data were collected via two ways, google form and paper survey distribution. We have taken (n=761) responses of survey questionnaires from the school students, (n=333) of university students and (n=108) from working women. We conducted the survey through random stratified sampling [78]. At the beginning of the survey we asked for consent from the participant. Assessing them on five key factors such as: password security, information security, device privacy, incident reporting and malware detection. Each five factor had a description at the beginning of the question, after the description of the factors such as definition of information security were added, then the questions were asked to the participants. The survey was conducted through in-person approach. We went to many urban areas school, rural semi and rural areas school across Bangladesh and distributed paper survey to the school students. We have taken the approval from the school authority to conduct the survey. The in-person availability helped the students to ask more about the questions, moreover by the in-person paper survey method we could also analyze their experience and behavior towards these survey questions. Furthermore, to gather the data of university students we mostly conducted the survey through google form. Sending the google form through a url (uniform resource locator), scan code, email and social media to the university students and then got a huge response from them. To collect the survey data from the working women we also applied the online google form method. Following these survey methods to all the three groups of participants, we collected our total responses from various areas of Bangladesh.

3.3.3 Selection of sample size

To collect the responses from the women we conducted random stratified sampling [78] so that we can ensure that the responses are unbiased and represent the large population of women. We rely on the availability of women in the practical data collection. We get most of the respondents from school students as we wanted to analyze the cyber security awareness from the early stage of their life from all areas (urban, semi rural, rural) of our country. It is important to mention that, in our country a large number of school students are prioritized to represent the future state of cyber security. Thus we emphasized on them. To select the sample size of the university students we targeted the students who are into using digital technology. And university students seems to use digital devices almost everyday in

their life. It reflects their higher involvement and stressed us to determine their cyber security awareness knowledge. For the selection of the sample size of working women, our survey data representation of working women is less compared to the students. World Bank reported [106] male working force is 64% whereas female working force is 36%. However, the responses we get from the working women helped us to analyze their cyber security behavior and awareness level. We have got many free-form responses("other") in the question from the participants. Following the random sampling method we continued our survey responses until no new information arose and identified that we are not getting any new or unique response from the free form ("other") option of the question.

3.3.4 Data Pre-processing for Survey

Beside the sample size n=1,202 in our study, at the beginning we did 6 pilot testing on our three targeted participants group. After that, we started collecting our survey. As we did a paper survey data collection on the high school students, we identified that many of the responses from the paper survey were not valid and many of the questions were not answered by some students. We considered those responses untrustworthy and invalid. Initially we got the school student's response of 36 from google form responses. After that, from urban, semi-urban and rural areas we got 778 responses through in-person paper survey. Around 53 numbers of data were discarded from the paper survey of school students. Following the removal of those data we got our total responses of 761 from survey and the rest of the responses of university students was (n=333) and working women were (n=108) which we collected through google form.

The extended elaboration on survey design can be found in Chapter 4 - Survey Design: Development and Distribution & detailed survey result in Chapter 5 - Survey Findings: Cybersecurity Awareness and Practice.

3.4 Data Collection for Interview

For our study, we have conducted interviews to find out more about the behaviour and knowledge of Bangladeshi women and their activity in the digital usage. Looking at these audiences in more detail, we focused on three different groups including high school students, university students, and working women. Moreover, in our survey questionnaire we set a optional question where we asked participant to provide their contact details if they are interested to join in our further interview part. It is important to mentioned that, we found a significant number of participants who voluntarily provided their contact details. For selecting the participants we followed the stratified sampling method [78] and snowball sampling method [1] to capture a broad range of perspectives. The process of participant selection was three months long, during which we were actively engaged with the participants.

3.4.1 Interview Participant

Participants were recruited via email shared on survey form, contact details, institutional networks, family connections, and efforts to ensure demographic diversity. Table 3.2 shows the distribution of interview participants.

High school students: To take the interviews, a proper consent has been taken from the high school students. There were 7 high school students in total and were between the ages of 13-20 years.

University students: We have also conducted interviews with the university students with their proper consent. There were 16 interviewees for university students and were between the ages of 19-24 years. By analyzing their responses, we gained insight into how young adults perceive and respond to cybersecurity threats and how their observations can inform better awareness campaigns and security practices.

Working Women: Lastly, the interview for working women was taken with the number of 7 women participants. Their age range was from 26-35 years. A proper consent was also taken from them with a consent form. We focused on understanding how their roles as working professionals influence their awareness on digital security, the challenges they face in implementing safety practices and their behaviour towards the cyber world.

Extended elaboration on interview design can be found in Chapter 6 - Interview Design: Development and Distribution & the result of interview in Chapter 7 - Interview Findings: Addressing Vulnerabilities and Strengthening Resilience.

Group	**Number of Participants**	**Percentage (%)**	**Age Range**
High School Students	7	23.33	13-20
University Students	16	53.33	19-24
Working Women	7	23.33	26-35
Total	30		-

Table 3.2: Demographics of Interview participants by group and age range

3.5 Data Analysis

For data analysis, we used Python as a medium and imported Panda, Numpy, Matplotlib, Seaborn, Scipy.stats, Sklearn.linear-model, Sklearn.model-selection and Sklearn.metrics, the following libraries initially for our analysis and visualisation.

The methods we used for data analysis are:

- **Descriptive statistics**: Descriptive analysis is used to summarize and describe the key attributes of the data, which reveals a clear understanding of its central measures and variability. By identifying mean score and standard

deviation we assess overall security knowledge and practice. Standard deviation measures the variability of response.

For each survey response a numeric value has been assigned, as min score 1 and max score 4. A higher mean score represents strong cyber security knowledge and practice while a low score indicates weaker cyber security awareness and practice of the participants.

- **Chi-Square Test of Independence**: Chi-Square test of Independence is used to test if 2 factors are associated with each other. It is determined by the critical value of 7.815. If the value is greater than the critical value, then test shows there is correlation between the factors or otherwise they are independent.
- **Logistic Regression**: Logistic Regression is used for modelling relationship between independent variable and dependent variable. It estimates the probability of an event occurring based on the data of the independent variable.
- **Multilevel Logistic Regression**: Multilevel Logistic Regression is used for modelling relationship between multiple variables.
  - **Heatmap**: Heatmap is a visualisation tool via which we represented the correlation of the factors in Multilevel Logistic Analysis. Heat maps uses colour gradient red to blue (high to low) to help to display the strength of relationship.
- **ANOVA Test**: ANOVA test is used to identify if there are any significant differences between groups.
- **Cronbach's Alpha**: Cronbach's Alpha is used to measure internal consistency, to test the reliability of a set of questions when measuring the same concept.

Chapter 4

Survey Design: Development and Distribution

In this chapter, we broke down the survey design of our research. We have discussed on key factors of cyber security and demographics which helped us to evaluate the cyber security awareness among Bangladeshi women. A detailed discussion over our selected demographic has been provided in this chapter along with descriptions of questionnaire topics, survey methods, statistical analysis and survey structure of our survey conduction.

4.1 Demographics

In this research we have conducted our survey on three different women groups in Bangladesh. Starting from, High school students, University students and Working women. We have asked each individual some required questions on the basis of these following categories:

- Age-range
- Residential zone
- Current level of study
- Academic field
- Job type
- Marital status

We conduct our survey using google forms for university student and working women. And for the high school students, the method was mostly paper survey. In the question we asked them about their residential status. By this, we came to know if they are from the urban, semi-rural or the rural area. Most of the high school students have the baseline understanding of cyber security knowledge. Though our goal was to determine self protection knowledge is yet known or unknown to them and whether the knowledge they have is adequate enough or not. From prior studies it is evident that, this group are more likely to associate themselves with cyber risks. On the other hand, university going students are also a huge part of

cyber crime victims in Bangladesh. Their perception in cyber security knowledge carries a huge significance in overall cyber awareness. Moving to, working women groups in Bangladesh, by depending on their job type, these women groups associate with technology in various ways. Women who work in the technical sector are more inclined to have some cyber security awareness knowledge than the women who don't. Therefore, exploring these dimensions, the method of assessing our participants' awareness has been conducted.

4.2 Survey Questionnaire

Based on the comprehensive literature reviews and relevant research studies, this research entitles essential five factors to examine on our targeted participants. Dividing into factors are following:

A) Password Security
B) Information Security
C) Device Privacy
D) Incident Reporting
E) Malware Detection

4.2.1 Questions Preparation

In our study, to understand the cyber security awareness among Bangladeshi women, we prepared a questionnaire that consists of 26 questions. We have set our questions in a way that everyone can easily understand. Such as, we have added the Bengali translation along with the English. It helped for all age groups of women to answer the question by a deep comprehension. At the end of all questions we have also added one open added question where participants can give their additional comments about cyber security knowledge. We settled all the 26 questions for three categories of people: high school students, university students and working women. The questions were set in five factors such as: Password security, information security, device privacy, incident reporting and malware detection. These five sectors are settled to determine their behavior and access the knowledge towards the cyber security awareness knowledge.

4.3 Choosing Factors: Question Breakdown and Analysis

We have divided our survey into 5 different factors and in total on each sector we had 26 different questions. In section A, first we gave a short discussion about "Password Security" and asked 5 questions on this sector. Password security is one of the foundational elements of protecting digital devices, personal information and accounts against cyber threats and unauthorized access. Good password practices are critical to the security of any information system [32].

Password management is a great factor since ineffective practices make users prone to some dangers such as hacking as well as data theft and others. Since multiple accounts are linked to digital devices, laxity on password discipline can cause extensive damage.

Our Questions related to password reusability probe how users expose multiple accounts to multiple breaches by reusing the same password across different accounts. Inquiries regarding incorporation of personal details in passwords assist in assessment of comprehensive strong password application. Then implementation of 2FA determines compliance to additional security measures. Question on password strength self-evaluations shows their reliability to their password habit. Moreover, knowing how users store their passwords gives insight into the various risks they expose themselves to. These help to understand missing knowledge in the cybersecurity field and illustrate the importance of enhancement of password creation, multi-factor authentication and management tools for the secure digital environment.

In section B, we asked about 3 different questions on "Information security". Confidentiality, integrity and availability of information are important concepts that require protection hence the need for information security. It helps to decrease the threats of phishing, viruses, trojans, malware and data loss in modern cybersecurity [44].

It has been observed that in last few years phishing attacks have grown rapidly posing a real threat to global security [47]. So that, the survey questions also range from participants' knowledge of phishing, capability of recognizing phishing scams and past involvement in cybersecurity training. As training enhances good security practices it is important to identify their involvments there. Assessing them on "informartion security" helps to determine the level of exposure to threats in the online environment and the corresponding levels of security. In summary, this sector tries to identify about security knowledge from women and inform future awareness initiatives.

For section C, there were about 4 questions on "Device Privacy" which indicates that device privacy gives individual's a measure by which they can regulate the accessibility of their personal devices and to avoid identity theft [56].

With the modern world full of advanced technologies, it is crucial to protect the device and data from unauthorized access. Knowing this concept, it is one of great important aspect to educating women about cybersecurity. In this factor, our first question is regarding device sharing with others and while the second is to tests women's ability to efficiently handle permissions of various applications. Understanding of threats from wi-fi is also necessary, thus we asked women about it as well.

Lastly, questions about protective measure is meant to test the device security choices from women. These questions described above cast light on the women's perception on device privacy and their efforts to make their devices more secure.

Consequently, in section D, we asked 4 questions which were about to know more details about the factor "Incident Reporting". The factor "Incident Reporting" is a critical component of cyber security where individuals and organizations are able to report cases of a cyber incident to the relevant authorities for legal purposes on prevention and better understanding on post-incident analysis [104]. Therefore we chose this factor, it has a significant function in gathering information that assists in enhancing security systems and fosters reporting behaviours. It is crucial to comprehend cybersecurity knowledge since. helps users to identify threats, act appropriately to cyber security incidents and have confidence in personal protection of their data.

The question asking about reporting cyberbullying incidents check the people's readiness to stand against online abuse and insecurity, securing hacked accounts and many more. Finally, experiences on managing cyber attack show the level of understanding security measures among the women and which areas may need for awareness creation. Collectively, these endeavour engender a more proactive approach to improving cyber security in the virtual sphere.

Lastly in our last section E, we wanted to know about the participants knowledge about "Malware Detection". There were a total of 4 questions on malware detection. Malware detection is the process of determining whether a given program has malicious intent or not [65]. Which is important for women to understand to ensure their digital safety. Our primary goals are to assess how much women know about their data protection, devices protection and increasing the user's awareness about cybersecurity.

Knowledge on how malware is detected is useful in a way that prepares users on how to make decisions when faced with them, as well as how best to stop them from spreading. Each question in the survey highlights important aspects of malware awareness such as awareness of signs of infection helps prevent its spread. Concern with downloading resource is also incorporate in this section. Questions on utilization of malware detection tools are provided to discover threats strengthen preventive measures. The application of anti-malware programs is evidence of continued vigilance.

In conclusion, malware detection is crucial for cybersecurity and it is crucial to be aware of potential threats and their prevention. Better understanding and response on malware can enhances security in women's digital spaces.

Why These Five Factors

Therefore, we select these five factors because they play a fundamental role in cybersecurity. Awareness on password security, information security, device privacy, incident reporting and malware detection should be identified as these are a way to enhance the security and privacy of the digital environment. Understanding these areas allows individuals the ability to protect themselves from cyber threats and risks. Assessing women through this factor allows us to identify and evaluate

women's preparedness in navigating the digital space safely. Employing these factors in our survey questions gives a valuable insight on women's knowledge, ability to defense and recognizing their vulnerabilities.

4.4 Sampling Method

To ensure a diverse study group, women from different demographics as well as from different educational backgrounds and professional experiences have been included in our study. This approach has taken to measure a wide range of cybersecurity awareness levels among participants. This study used a stratified random sampling method [5] commonly known as convenience sampling [85] to efficiently select participants. For high school students, we reached out to some of them through google form but the majority of the high school student's data was collected through paper surveys distributed at their schools by taking permission from the school authority. For university students and working women, we reached to them using social networks through google forms. The sampling method we have used there not only ensured diversity of participants but also helped us to understand how different social and educational backgrounds affect cybersecurity awareness and behavior. By grabbing different perspectives from a wide range of participants with different levels of digital experience, the study gives a clearer picture of what makes people more vulnerable to cybersecurity threats and how well different awareness efforts work.

4.5 Survey Distribution

To achieve a wide audience, the survey was distributed online and offline. For the high school participants, we took both google form method and paper survey in case of restricted internet availability and for the sake of fairness to younger participants. In the case of university students and working women, an online questionnaire was developed using google forms. This method was chosen to provide easy accessibility and convenience, as these individuals are more familiar with digital platforms and more willing to participate in online surveys. The distribution of google forms also allowed for faster response times and easier collection of responses. Using both digital and physical survey methods, our study aims to minimize accessibility barriers and provide a more diverse and accurate data-gathering approach.

The result of survey design is comprehensively discussed in Chapter 5 - Survey Findings: Cybersecurity Awareness and Practice.

4.6 Survey Structure

In our thesis we followed several steps to complete our survey. Here the flow diagram of survey design is given in Figure 4.1

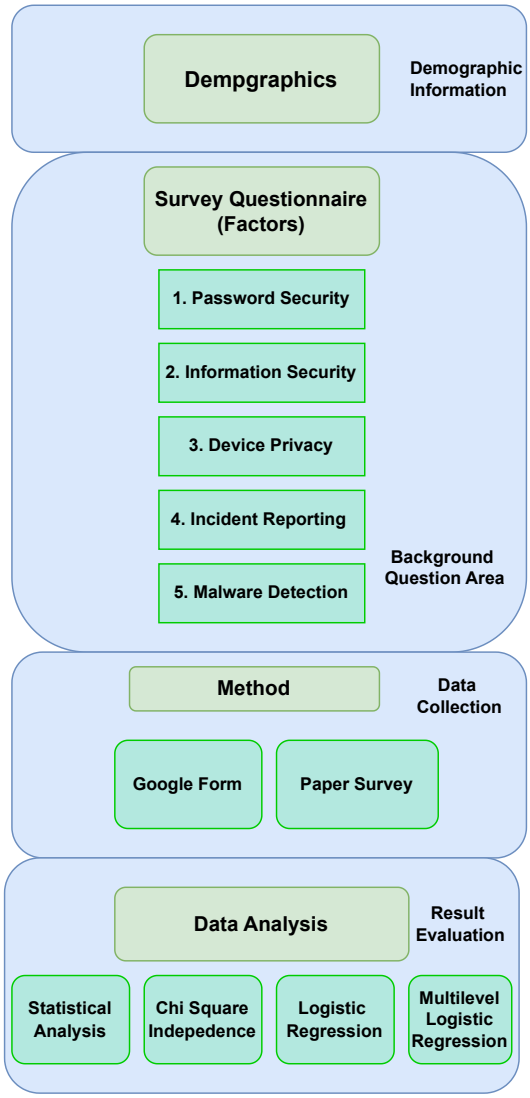

Figure 4.1: Survey structure

Following this structure, our survey has conducted taking on demographic information as the baseline criteria for participant inclusion. Subsequently, the survey questions are proposed to the chosen participants. Collecting all the response systematically, we performed data analysis to examine the obtained responses.

Chapter 5

Survey Findings: Cybersecurity Awareness and Practice

This chapter presents the findings from survey analysis across our three groups of demographics. Exploring through five keys of cyber security such as, password security, information security, device privacy, incident reporting and malware detection, we analyse knowledge and practice of them. Analysing thoroughly on these factors, we aim to address the cyber security awareness level of women.

5.1 Demographics

This section provides detailed description and breakdown of demographic of survey participants. The distribution of three groups of participants: high school student, university student and working women. An overview of participants background including age, academic, job status, grade level and geographic representation is comprehensively discussed here.

5.1.1 High School Students

A total of 761 students from high school participated in the survey. Table 5.1 shows the overall result of high school students' demography. As we set the age ranged from 12 to more than 43 years, the mean age = 15.36 years and standard deviation. = 2.02 is for high school students. The students voluntarily participated in this study. Out of 761 participants the majority age group 12-15 years (n=410) is the majority 53.8%, the rest of the participants are in the age-group 16-19 years (n=349) 45.7% and 20-23 years (n=2) 0.4%. The field of their study contributed across science, business studies, arts/humanities and others. From the science background 59.5% students participated, 10.3% from business studies, Arts/Humanities 3.4% and 26.8% reported that their field of study is not decided yet. The current class/grade they reported is (n=68) 8.80% participant fall in the range of class 6-7, (n=448) 59.0% from range of class 8-10, (n=224) 32.06% participant studies in class range of 11-12 and, along with these 1 student reported as a university admission candidate. Students from different areas had contributed, among them a huge participant of 70.7% were from urban areas, 22.2% from semi urban areas and 7.2% students from rural areas.

Distribution	Number of participants	Percentage (%)
Age Range		
12-15 years	410	53.8
16-19 years	349	45.7
20-23 years	2	0.4
Field of Study		
Science	452	59.5
Business Studies	78	10.3
Arts/Humanities	26	3.4
Undecided	205	26.8
Class/Grade		
Class 6-7	68	8.80
Class 8-10	448	59.0
Class 11-12	244	32.06
Admission candidate	1	0.1
Geographic Area		
Urban	538	70.7
Semi-urban	168	22.1
Rural	55	7.2
Age Statistics		
Mean age	15.36 years	
Standard deviation	2.02	

Table 5.1: Demography of the 761 high school students.

5.1.2 University Students

From the group of university students we obtained a survey response from 333 participants. Table 5.2 shows the overall result of university students' demography. We got students from 16-31 age group and a mean age = 22.03 years for the university students and standard deviation = 1.76. It shows that more of the university students are from the age range of 22-23 years (n=264). The participants' fields of study reached across engineering, law, pharmacy and many more. Notably, the students came from the engineering department. A percentage of 44.14% engineering students, 10.5% from pharmacy, 9.30% from business, 6.0% from medical sector, 5.70% from law and arts and the rest of the percentage from other respective departments. In terms of resident area, the majority of students 92.7% (n=309) from the urban area, 5.10% of semi urban (n=17) and only 2.10% (n=7) from the rural area.

Distribution	Number of participants	Percentage (%)
Age Range		
16-19 years	6	1.80
20-23 years	264	79.3
24-27 years	61	18.3
28-31 years	2	0.60
Field of Study		
Engineering	147	44.14
Pharmacy	35	10.5
Business	31	9.30
Medical	20	6.00
Law	19	5.70
Arts	19	5.70
Other	62	18.6
Geographic Area		
Urban	309	92.7
Semi-urban	17	5.10
Rural	7	2.10
Age Statistics		
Mean age	22.21 years	
Standard deviation	1.76	

Table 5.2: Demography of the 333 university students.

5.1.3 Working Women

The result of working women responses shows that a total of (n=108) participants. Table 5.3 shows the whole result of working women's demography. The highest number of responses are obtained from the age group of 40-43 (n=23), more than 43 (n=22). The result of mean age shows, mean=36.05 years, standard deviation = 7.80. Among all participants 75.9% reported as married, 22.2% as single and 1.85% reported as divorced. According to their area of employment we got various results such as 23.1% of women belong to gov/private job holders, 17.6% from academia/education, teachers, tutor, principle, 15.7% of the medical sector, 16.7% from the banking/accounting sector, 11.1% from the engineering sector. Additional sector contains rest of the percentage. To analyze the reside area we got the highest response from the urban area, about 95.37% of women responded from urban area and rest of the women are from semi urban and rural area.

Distribution	Number of participants	Percentage (%)
Age Range		
40-43 years	23	21.3
More than 43 years	22	20.4
Other age groups	63	58.3
Marital Status		
Married	82	75.9
Single	24	22.2
Divorced	2	1.85
Employment Sector		
Gov/Private Job Holders	25	23.1
Academia/Education	19	17.6
Medical Sector	17	15.7
Banking/Accounting Sector	18	16.7
Engineering Sector	12	11.1
Other	17	15.7
Geographic Area		
Urban	103	95.37
Semi-urban	3	2.77
Rural	2	1.85
Age Statistics		
Mean age	36.05 years	
Standard deviation	7.80	

Table 5.3: Demography of the 108 working women participants.

5.2 Password Security

We have set five questions to assess the understanding of cyber security awareness among our three targeted groups of women. These questions particularly evaluate how they manage and protect their online identities. A descriptive analysis is performed to analyse the cyber security awareness knowledge of them. For each response we assigned a numeric value, here we set the min score as 1 and max score 4. A higher mean score indicates better cyber security knowledge and good practice and lower score suggests low cyber security awareness and bad practice of the participants.

5.2.1 High School Student

When we asked the high students about their tendency to use the same password for multiple accounts, the result shows a mean score of = 3.19, standard deviation = 0.99. As a higher score indicates a better behaviour of not reusing the same password, it reveals that high school students have a better cyber security habit by avoiding the password reusing for multiple accounts. Moreover, In the response of using personal information while creating the password, through the descriptive analysis the result shows a mean score: 2.74 and standard deviation = 1.09. In this analysis we got a moderate mean score which suggests that respondents are less aware about the potential risk of using personal information on their password

creation. Our analysis shows that nearly 40% of the students have poor practice in password creation. Furthermore on the third question of asking about the consistency in activating Two-Factor Authentication (2FA) it is shown in Table 5.4 a low mean score = 2.20 and standard deviation = 1.14. This analysis suggests that 60% of students never and rarely use 2FA and only 19% of students use 2FA. The overall results portray that low awareness of cyber security. Figure 5.1 shows the password security analysis result for high school Students. On analyzing the question which method students generally follow to keep password safe, students mostly responded on "memorizing the password" 56.1% and 25.0% reported they "securely note down" their password. Lastly, on the analysis of confidence level, they consider their passwords safe and secure where we got a result of mean = 2.99 st.dev. = 0.85 of only 26.15% students reported as moderately confident.

Description	**Never**	**Rarely**	**Mostly**	**Always**
Password Reuse Across Multiple Accounts				
Responses	382	215	87	77
Mean	3.19			
Standard Deviation	0.99			
Min-Max	1-4			
Result	Better Knowledge			
Use of Personal Information in Passwords				
Responses	237	234	146	144
Mean	2.74			
Standard Deviation	1.09			
Min-Max	1-4			
Result	Moderate Knowledge			
Consistency in Activating Two-Factor Authentication (2FA)				
Responses	290	174	151	146
Mean	2.20			
Standard Deviation	1.14			
Min-Max	1-4			
Result	Low Knowledge			

Table 5.4: Descriptive analysis results on password security for high school students

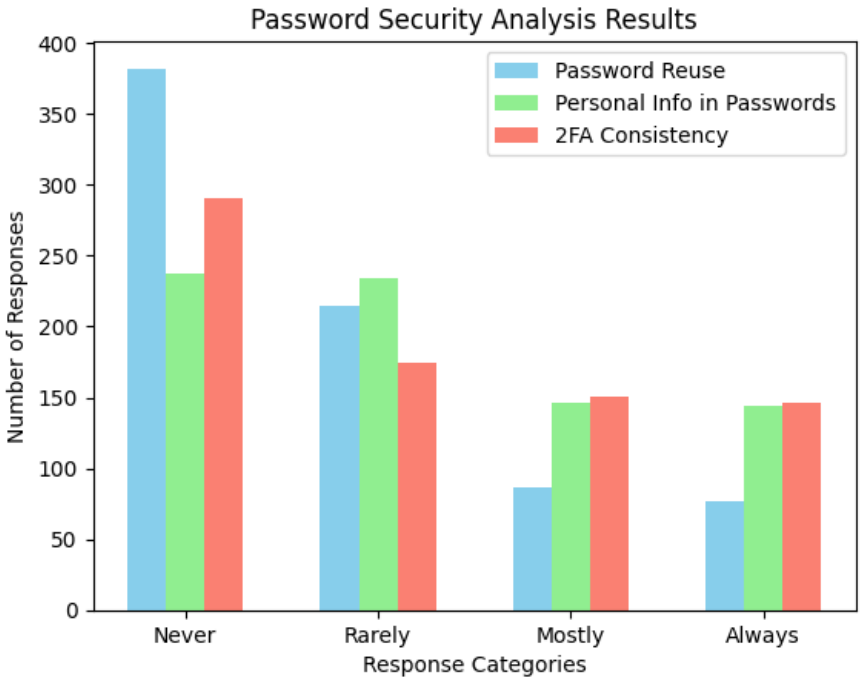

Figure 5.1: Result of password security for high school student

5.2.2 University Student

When we analyzed the same question to the university students, in response to their tendency to use the same password for multiple accounts a mean score = 2.66 and standard deviation = 0.96 of results we got. This mean score indicates that the majority of university students tend to avoid using the same password for across accounts. This represents a moderate level awareness of the risk related with password reuse. Table 5.5 shows the password security analysis result for university students. The result shows participants are somewhat likely to use personal information while creating passwords, a score of mean = 2.83 and standard deviation. = 0.93. But again still a significant number of students (n=124) mostly and always reported as using personal information. The consistency in activating 2FA shows the result of mean score = 3.11, standard deviation = 0.83. This results indicates that 76.2% of university students always and mostly use 2FA, on the other hand 23.72% rarely or never use it. Furthermore, managing their password 43.2% "memorized" and 20.4% university students reported "securely note down" to keep their password safe. Lastly, we analyzed the confidence level of feeling their passwords are safe and secure. In the response of this question, we got a result of mean = 3.02, standard deviation = 0.68 and 30.63% of students are being of a moderate to good level confidence.

Description	Never	Rarely	Mostly	Always
Password Reuse Across Multiple Accounts				
Responses	81	93	125	34
Mean	2.66			
Standard Deviation	0.96			
Min-Max	1-4			
Result	Moderate Knowledge			
Use of Personal Information in Passwords				
Responses	94	115	98	26
Mean	2.83			
Standard Deviation	0.93			
Min-Max	1-4			
Result	Moderate Knowledge			
Consistency in Activating Two-Factor Authentication (2FA)				
Responses	10	69	130	124
Mean	3.11			
Standard Deviation	0.83			
Min-Max	1-4			
Result	Better Knowledge			

Table 5.5: Descriptive analysis results on password security for university student

5.2.3 Working Women

To analyze the password security awareness knowledge of working women we found a mean score of 2.69, standard deviation = 1.07 for the password reuse across multiple accounts. This shows that most of the women never to rarely reuse their passwords, which shows a better cyber security practice. On analyzing the answers of using their personal information, it shows a mean score of 2.59 and standard deviation = 1.00 that indicates that the awareness level of using personal information while creating passwords is low to moderate. From the Table 5.6 it can be seen mean score = 2.55, standard deviation = 1.07 result has come out for using the 2FA to secure the account. This mean score reveals that they mostly use it, which falls into on average respondents' somewhat inconsistent on cyber security practice. In managing their passwords, working women mostly use the method of "memorizing the password" 47.2% and their confidence of secure and safe password shows a result of mean score= 2.79 and st.dev. = 0.89, Figure 5.2 shows working women's moderate confidence in password security and strength.

Figure 5.2: Result of confidence level over password security (working women)

Description	Never	Rarely	Mostly	Always
Password Reuse Across Multiple Accounts				
Responses	31	32	26	19
Mean	2.69			
Standard Deviation	1.07			
Min-Max	1-4			
Result	Moderate Knowledge			
Use of Personal Information in Passwords				
Responses	24	33	34	17
Mean	2.59			
Standard Deviation	1.00			
Min-Max	1-4			
Result	Moderate Knowledge			
Consistency in Activating Two-Factor Authentication (2FA)				
Responses	25	22	38	23
Mean	2.55			
Standard Deviation	1.07			
Min-Max	1-4			
Result	Moderate Knowledge			

Table 5.6: Descriptive analysis results on password security for working women

5.2.4 Hypothesis 1: Testing

H1: Women who reuse passwords across accounts might be less likely to consistently use 2FA.
For the analysis of this hypothesis, the relevant questions are:

- For multiple accounts (personal/university/work-related), do you have the tendency to use the same password?

- How consistent are you in activating two-factor authentication (2FA) to secure your accounts?

Upon these questions, we are using chi-square test of independence where the value ≥ 7.815, we can conclude that there is a significant correlation between the factors or otherwise, it is independent. The p value signifies whether the data is statistically

significant. The degree of freedom represent how the the data had a number of independent values and were not limited to binary responses. It is calculated by:

$$\text{df} = (\text{number of rows} - 1) \times (\text{number of columns} - 1)$$

and furthermore, we took the aid of the library to call chi2 contingency function to provide the analysis of the hypothesis on our targeted groups.

At first, we test the Hypothesis 1 for our High school student.

2FA	**Always**	**Mostly**	**Never**	**Rarely**
Same Password - Always	18	17	80	31
Same Password - Mostly	12	14	67	58
Same Password - Never	39	34	175	42
Same Password - Rarely	8	22	60	84

Table 5.7: Contingency table of same password vs 2FA (raw counts)

Furthermore, we can observe from the contingency Table 5.7 if our hypothesis of High school students who reuse passwords are less likely to use 2FA. For easier understanding, we converted it to percentage.

2FA	**Always**	**Mostly**	**Never**	**Rarely**
Same Password - Always	12.33%	11.64%	54.79%	21.23%
Same Password - Mostly	7.95%	9.27%	44.37%	38.41%
Same Password - Never	13.45%	11.72%	60.34%	14.48%
Same Password - Rarely	4.60%	12.64%	34.48%	48.28%

Table 5.8: Contingency table of same password vs 2FA

Then we compared the percentage of combination From Table 5.8 of 2FA(Never, Rarely) and same-password (Always, Mostly) against 2FA(Always, Mostly) and Same-Password (Never, Rarely) to figure out the likeliness of students reusing passwords and not using 2FA. Therefore,

- 2FA (Never, Rarely & Same-Password (Always, Mostly) = 42.39
- 2FA (Always, Mostly & Same-Password (Never, Rarely) = 158.8

From comparing, we see high school students are most likely to use 2FA while not reusing password hence we are say, our hypothesis is not valid in this case .

Furthermore, by analyzing Chi square result which came as: Chi-squared value: 79.06, P-value: 2.48×10^{-13} and Degrees of freedom: 9.
We see Chi-square value is greater than 7.19 which rejects the notion that the two factors are independent of each other. The P-value: 2.48×10^{-13} is lesser than 0.05 hence that data are statistically significant, hence the 2FA and same-password are dependent upon each other and there is a significant relationship between two.

2FA	Same Password Always	Mostly	Never	Rarely
Always	11	49	30	34
Mostly	16	45	34	35
Never	0	3	4	3
Rarely	7	28	13	21

Table 5.9: Contingency table with frequencies

Secondly, we test Hypotheis 1 For University Student

Furthermore, we can observe from the contingency Table 5.9 if our hypothesis of university students who reuse passwords are less likely to use 2FA. For easier understanding, we converted it to percentage.

2FA	Same Password Always	Mostly	Never	Rarely
Always	8.87%	39.52%	24.19%	27.42%
Mostly	12.31%	34.62%	26.15%	26.92%
Never	0.00%	30.00%	40.00%	30.00%
Rarely	10.14%	40.58%	18.84%	30.43%

Table 5.10: Contingency table: use of same password vs. 2FA (with percentages)

Then we compared the percentage from Table 5.10 of combination of 2FA (Never, Rarely) and same-password (Always, Mostly) against 2FA (Always, Mostly) and same-password (Never, Rarely) to figure out the likeliness of university students reusing passwords and not using 2FA. Therefore,

- 2FA (Never, Rarely & Same-Password (Always, Mostly) = 80.71
- 2FA (Always, Mostly & Same-Password (Never, Rarely) = 104.6

From comparing, we see university students are most likely to use 2FA while not reusing password hence we are say, our hypothesis is not valid in this case .

Furthermore, by analyzing Chi square result which came as: Chi-squared value: 4.82 P-value: 0.849 Degrees of freedom: 9 Since chi is less than 7.19, it means the factors 2 FA and reuse passwords across accounts share no correlation and are independent of each other. As the P value is greater than 0.05, it's not statistically significant for our University Student group.

Lastly, we test the Hypothesis 1 for Working Women.

Furthermore, we can observe from the contingency Table 5.11 and 5.12 shows if our hypothesis of working women who reuse passwords are less likely to use 2FA. For easier understanding, we converted it to percentage.
Then we compared the percentage of combination from Table 5.11, 5.12 of 2FA(Never, Rarely) and same-password(Always, Mostly) against 2FA(Always, Mostly) and same-password (Never, Rarely) to figure out the likeliness of working professional reusing passwords and not using 2FA. Therefore,

2FA	Same Password Always	Mostly	Never	Rarely
Always	3	7	7	6
Mostly	5	6	15	12
Never	7	6	3	9
Rarely	4	7	6	5

Table 5.11: Contingency table of 2FA and same password usage

2FA Usage	Same Password Always	Mostly	Never	Rarely
Always	13.04%	30.43%	30.43%	26.09%
Mostly	13.16%	15.78%	39.47%	31.58%
Never	28.00%	24.00%	12.00%	36.00%
Rarely	18.18%	31.82%	27.27%	22.73%

Table 5.12: Percentage table of 2FA and same password usage

- 2FA(Never, Rarely & Same-Password (Always, Mostly) =101.98
- 2FA(Always, Mostly & Same-Password (Never, Rarely)=127.55

From comparing, we see working women are most likely to use 2FA while not reusing password hence we are say, our hypothesis is not valid in this case .

Furthermore, by analyzing Chi square result which came as: Chi-squared value: 9.10 P-value: 0.427 Degrees of freedom: 9 The chi value is greater than 7.19 which suggests the variables are dependent upon each other but since the P value is greater than 0.05, the data is not statistically significant hence it was said that there is no statistically significant association between "2FA usage" and "Same Password usage". Therefore, they can be considered independent of each other.

5.3 Information Security

In the information security section, we have setted 3 survey questions. These three questions focus on the fundamental knowledge of the possible threats while using digital devices. Moreover this sector analyzes the practical ability of recognizing cyber risks. All together the results portray the overview of women cyber security awareness knowledge in information security factor. For each response a numeric value has been assigned, as min score 1 and max score 4. A higher mean score reflects strong cyber security awareness and practice while a low score indicates weaker cyber security awareness and practice of the participants.

5.3.1 High School

Analyzing the first question, which asks the students whether they are aware of phishing, we got a mean score = 2.31, standard deviation = 1.11. Among the total participants 33% students never heard of phishing and 17.6% claim to know about it. This mean score suggests that students are either unaware or somewhat aware of phishing and overall it portrays a low knowledge of phishing. Table 5.13 shows

information security analysis result for high school students.
Moreover when the students were asked to identify a phishing example it shows a mean score = 2.09 and standard deviation = 2.29. This average mean score shows that the students have low understanding of phishing. Around 51% of students responded that "I have no Idea." As the result indicates that over half of the students are unable to identify phishing and only 30% correctly identified, significant students are vulnerable to phishing attacks and have less knowledge of phishing.
Lastly, the students were asked about have they ever attended any cyber security awareness training/seminar/workshop, the result shows a very low percentage of 11.4% have attended and 60.4% respondents that never attended and wished to attend in future.

Description	**Responses**	**Mean**	**SD**	**Result**
Do you know Phishing?				
Never heard of Phishing	254	2.31	1.11	Low Knowledge
Somewhat know Phishing	220			
Not sure	153			
Fully Aware	134			
Which is an example of Phishing?				
No idea	392	2.09	2.29	Low Knowledge
Email Link (correct one)	233			
Total Incorrect Identification	136	-	-	-
Cybersecurity Awareness Training Attendance				
Attended	11.4%			
Wish to attend	60.4%	-	-	-

Table 5.13: Descriptive analysis results on information security among high school students

5.3.2 University Student

To assess the university student's knowledge about phishing we got a result of mean score = 2.76, standard deviation = 1.11, most of the university student respondents said that they have general ideas about phishing. On the other hand, on recognizing the phishing example, most of the students seem to detect the phishing correctly, from the Table 5.14 it can be seen mean score of 3.52 and st.dev.= 2.08. Concurrently (n=204) participants could correctly identify and (n=60) could not answer correctly, (n=69) reported that they have no idea of phishing. This suggests that, significant portion of respondents have good knowledge on phishing threats. However there is still a considerable portion of university students who either misunderstood the example of phishing or have no knowledge of phishing. Lastly, we analyze their answers of if they have ever attended any awareness training/seminar/workshop; where half of the respondents 52.0% responded with no and would like to attend in future.

Description	Responses	Mean	SD	Result
Do you know Phishing?				
Never heard of Phishing	68	2.76	1.11	Moderate Knowledge
Somewhat know Phishing	104			
Not sure	51			
Fully Aware	110			
Which is an example of Phishing?				
No idea	69	3.52	2.08	Better Knowledge
Email Link (correct one)	204			
Total Incorrect Identification	60			
Cybersecurity Awareness Training Attendance				
Attended	11.4%			
Wish to attend	52.0%			

Table 5.14: Descriptive analysis results of information security on university student

5.3.3 Working Women

On the investigation of information security knowledge of working women, a result of mean score = 2.19, standard deviation = 1.22 has emerged on the question of whether they know about phishing. Among a total of (n=108) respondents, (n=48) respondents shared that they never heard of phishing and only (n=24) respondents says that they know about phishing and aware of all danger. Furthermore, (n=36) respondents respond that they have somewhat and not a sure idea about phishing. While accessing the phishing example, a mean score of 2.28 and standard deviation = 2.31 has appeared. As it can bee seen from Table 5.15 the majority of respondents have no idea about recognizing phishing. About 42.59% (n=46) women had no idea, 38.89% (n=42) were correct about the answer, 18.52% (n=20) were wrong about the answer. The working women also never attended and showed desire to attend cyber security training/workshop/seminar about 51.9% respondent.

Description	Responses	Mean	SD	Result
Do you know Phishing?				
Never heard of Phishing	48	2.19	1.22	Low Knowledge
Somewhat know Phishing	21			
Not sure	15			
Fully Aware	24			
Which is an example of Phishing?				
No idea	46	2.28	2.31	Low Knowledge
Email Link (correct one)	42			
Total Incorrect Identification	20			
Cybersecurity Awareness Training Attendance				
Attended	15.7%			
Wish to attend	51.9%			

Table 5.15: Descriptive analysis results on information security of working women

5.4 Device privacy

In the Device privacy sector, the survey included four questions. To analyze the responses we got the results of women's practice behaviors regarding their device, which is a key component of cyber security awareness knowledge. All together the responses of the device privacy indicate a comprehensive understanding of participants' cyber security awareness. The responses are also mapped with a score of min 1 to max 4, where lower scales portray less awareness and habit and higher scores show stronger cyber security awareness knowledge and habit.

5.4.1 High School

First of all, on the question of whether they share their smartphone with others we got a result of mean score = 2.74 and standard deviation = 1.03. Moreover on analyzing the question of reviewing or adjusting the app permission, a mean score = 2.62 and st.dev. = 0.95. This mean score suggests that there is a moderate level of awareness in terms of app permission review, which can be seen from the Figure 5.3 and Table 5.16. The students were also asked about their awareness on using public wi-fi. The result shows that mean score = 2.60 and standard deviation = 1.06. About 36.7% (n=279) of students are unsure about taking precautions while using public wi-fi. Lastly, we wanted to find out the strategy they use in protect their device from unauthorized access and got a result of 50.1% students use strong password/pin and 6.0% reported they do not use any protection on their device.

Description	**Never**	**Rarely**	**Sometimes**	**Frequently**
Smartphone Sharing	217	245	180	119
Mean (St. Dev.)	2.74 (1.03)			
Reviewing App Permissions	114			134
Mean (St. Dev.)	2.62 (0.95)			
Public Wi-Fi Risk Awareness				
Mean (St. Dev.)	2.60 (1.06)			
Device Protection Strategy	Strong Strategy: 50.1%, No protection: 6.0%			

Table 5.16: Descriptive analysis result of device privacy for high school student

5.4.2 University Student

To analyze the habit of device sharing of university students, a mean score = 2.99, standard deviation = 0.76 has been revealed in Table 5.17. It proves that they have a better habit of not sharing not sharing smartphone. When the university students were asked about reviewing or adjusting their permission after app installation, we got a result of mean score = 2.61, standard deviation = 0.86. This result portrays that average level of awareness. A mean score = 2.73 and standard deviation = 0.90 has emerged on the answer of their awareness while using public wi-fi, 39.3% of students admit that they are aware but not always take precautions, 28.8% of students are somewhat aware but unsure of the precautions and 9% of students are not aware at all and 21.32% response on they are fully aware and take precautions.

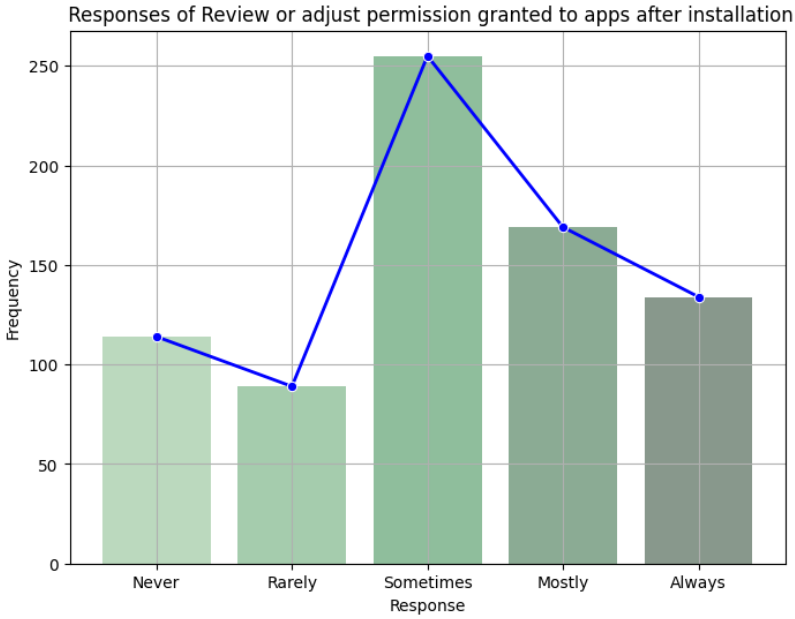

Figure 5.3: Reviewing or adjusting permission granted to apps after installation (high school students)

The strategy they mostly use about 48.0% students protect devices from unauthorized access by using both password and biometric.

Description	**Never**	**Rarely**	**Sometimes**	**Frequently**
Smartphone Sharing	89	158	80	6
Mean (St. Dev.)	2.99 (0.76)			
Reviewing App Permissions	31			50
Mean (St. Dev.)	2.61 (0.86)			
Public Wi-Fi Risk Awareness				
Mean (St. Dev.)	2.73 (0.90)			
Device Protection Strategy	Strong Strategy: 48.0%, No protection: 3.6%			

Table 5.17: Descriptive analysis result of device privacy for university student

5.4.3 Working Women

On the question of whether they share their device, the working women have responded by sharing their smartphone with others of mean score = 2.78 and standard deviation = 1.04. Figure 5.4 shows the practice of participants' device sharing results with others. This result indicates the have moderate level habit of sharing smartphones. A low mean score of = 2.28 and standard deviation = 0.98 has shown that most of the participants do not have the practice of adjusting the permission granted apps after installation. On the other hand, analyzing the awareness of the risk of using public wi-fi a mean score = 2.24 and st.dev. = 1.05 has come in the result. About 31.48% participants seem to not be aware at all, 27.78% are somewhat aware but unsure of precautions, 25.93% are aware but not always taking precautions and only 14.81% of participants are fully aware and take precautions. Use of

a strong password and pin was the most reported method of working women, about 42.6% and where from the Table 5.18 it can be seen 36.11% use both password and biometrics where 5.0% participant takes no protection in their device protection strategy.

Description	**Never**	**Rarely**	**Sometimes**	**Frequently**
Smartphone Sharing	32	37	22	17
Mean (St. Dev.)	2.78 (1.04)			
Reviewing App Permissions	27			11
Mean (St. Dev.)	2.28 (0.98)			
Public Wi-Fi Risk Awareness				
Mean (St. Dev.)	2.24 (1.05)			
Device Protection Strategy	strong strategy: 36.1.1%, No protection: 5.0%			

Table 5.18: Descriptive analysis result of device privacy for working women

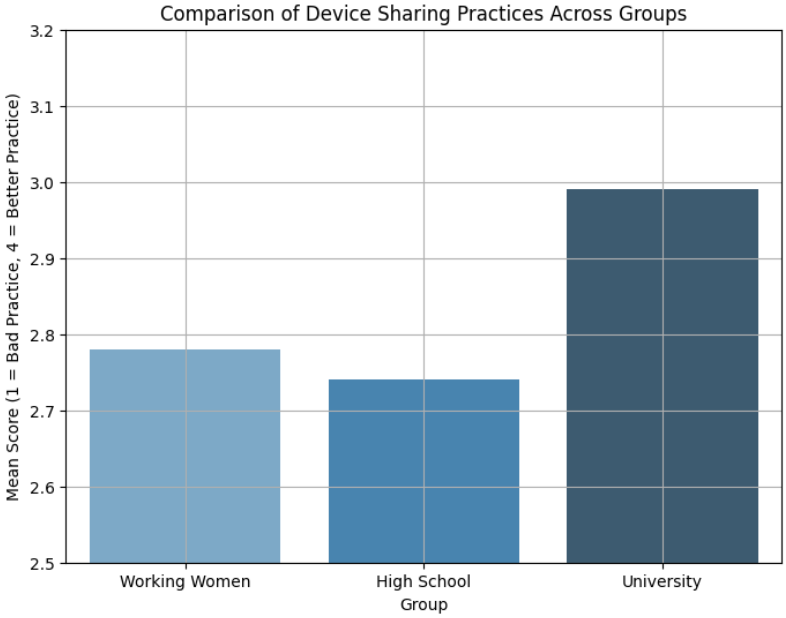

Figure 5.4: Practice of device sharingnwith others (all three group)

5.5 Incident Reporting

In the incident reporting sector the survey had three questionnaires. The response of the question has provided us an understanding of participants knowledge and situational awareness while facing any digital problem. All together, the result shows us a cyber security awareness on this sector. The responses were assigned with a numeric value, as min score 1 and max score 4. A higher mean score reflects strong cyber security awareness and practice while a low score indicates weaker cyber security awareness and practice of the participants.

5.5.1 High School Student

For the first question participants were asked about have they ever experienced and report an cyber bullying incident, the result shows a percentage of 47.1% students has experienced cyber bullying, 15.0% witnessed and 37.2% never experienced or witnessed it. Among all participants only 18.3% reported those incidents.
In another question of asking the students, in case of any security breaches, whether they know the steps of securing steps. We got a mean score of 2.79 and a standard deviation of 0.97 for this answer. About 28.2% students responded that they know exactly what to do to be secure and take immediate action and 33.4% respond that they have a general idea but need more information on specific action. This result represents that most of the students have an average level of knowledge in which action to take in this case.
Lastly, the survey questionnaires were about to analyze the students' confidence level of handling cyber attacks. A result shows a mean score of 2.77 and standard deviation = 1.04. This mean score indicates that students are moderately confident in handling cyber attacks. Only (n=59) 7.75% students among (n=761) students has reported that they are extremely confident. Whereas, (n=128) 16% students stated that they are not confident at all.

5.5.2 University Student

To analyze the responses that university students have ever experienced a cyber bullying and report it 41% students reported that they have experienced cyberbullying, 25.5% witnessed and 31.9% never experienced or witnessed it. Among all participants only 29.4 % reported the cyberbullying incidence or multiple times. In the response of their action to take while any security breaches happens, the results show a mean score = 3.10 and standard deviation = 0.80. This result shows that, they have somewhat well knowledge of protection. About 43.8% give an answer on "I have general idea, but need more specific information", where also 34.2% responses are on "I know exactly what to do and would take immediate action." This answer portrays a moderate level cyber security awareness knowledge. Furthermore, about the confidence level in ability to handle cyber attack, university students have a mean score = 2.80 and st.dev. = 0.93. This mean score indicates that they have an average confidence level in themselves. This is important to mention that among the total of (n=333) participants, (n=42) 12.61% respondents reported that they are not confident at all and (n=57) 17.11% participants are slightly confident in their ability to handle cyber attacks. Where only (n=20) 6% participants response on extremely confident.

5.5.3 Working Women

To assess the response of working women, on the the question of whether they have ever experienced and reported cyberbullying incident where 36.9% women experienced cyber bullying and 36.1% have reported on never having experienced it, 20.3% have reported the cyberbullying incident once or multiple time. In their response, to actions taken during any security breach on the password, device or social media account we got a mean score = 2.53 and standard deviation = 0.96. It indicates that on average women fall in between moderate to limited knowledge in terms of

which action to take. Working women came across as less confident in their ability to handle cyber attacks such as a score of mean = 2.56, std.dev. = 1.15. In the total of (n=108) participants, (n=30) 27.78% reported as not confident at all, (n=15) 13.89% reported as slightly confident, (n=35) 32.41% participants are moderately confident and (n=22) 20.37% are mostly confident. It is noticeable that only (n=5) 4.62% are extremely confident.

5.5.4 Hypothesis 2: Testing

H2: "The confidence in women's ability to handle cyber-attacks correlates with reporting cyberbully incidents?"
For the analysis of this hypothesis, the relevant questions are:

- Have you ever reported a cyberbullying incident?
- Are you confident in your ability to handle cyber attacks?

Upon these questions, we using logistic regression to analyses the data to see if confidence does affect the probability of reporting cyberbully incidents. The logistic regression also provides us with a classification report where the precision shows the positive ratio results of each prediction while Recall shows the actual positive ratio within the dataset. F1 score is the harmonic mean of both precision and recall while the support is actual count of each class in the dataset where the class is the target variable which represents positive and negative venture the accuracy represents the overall accuracy of used model.

Firstly, we test the Hypothesis 2 for our High school student.

Class	Precision	Recall	F1-score	Support
0.0	0.80	1.00	0.89	184
1.0	0.00	0.00	0.00	45
Accuracy			0.80	229
Macro avg	0.40	0.50	0.45	229
Weighted avg	0.65	0.80	0.72	229

Table 5.19: Classification report

The result of the logistic regression by the model:
Coefficient (Impact of Confidence): [[0.14282214]] Intercept: [-1.93490061]
The coefficient of confidence is 0.14282214 which is positive; it indicates with increase of confidence, likelihood of reporting of cyberbullying incidents would increase. The Y-intercept represents when confidence=0, as the intercept is negative, the probability of success would be low. Table 5.19 shows the classification report for high school students.

If we calculate the probability of reporting when *Confidence* is high, using the logistic function then the formula is:

$$P(y=1) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 \times \text{Confidence})}} \tag{5.1}$$

Where:

- $\beta_0 = -1.9349$ (Intercept)
- $\beta_1 = 0.1428$ (Coefficient for Confidence)
- Confidence = 5 (High Confidence Level in Likert scale)

$$\begin{aligned} P(y=1) &= \frac{1}{1+e^{-(-1.9349+0.1428\times 5)}} \\ &= \frac{1}{1+e^{-(-1.9349+0.714)}} \\ &= \frac{1}{1+e^{-(-1.2209)}} \\ &\approx \frac{1}{1+0.2945} \\ &\approx \frac{1}{1.2945} \\ &\approx 0.2278 \end{aligned}$$

Thus, the probability of reporting when *Confidence* is high (at a value of 5) is approximately $P(y=1) \approx 0.2278$ or 22.78%. As opposed to when confidence is 0

$$P(y=1) = \frac{1}{1+e^{-(\beta_0+\beta_1\times \text{Confidence})}} \tag{5.2}$$

Where:

- $\beta_0 = -1.9349$ (Intercept)
- $\beta_1 = 0.1428$ (Coefficient for Confidence)
- Confidence = 0

therefore:

$$\begin{aligned} P(y=1) &= \frac{1}{1+e^{-(-1.9349+0.1428\times 0)}} \\ &= \frac{1}{1+e^{-(-1.9349)}} \\ &\approx \frac{1}{1+6.919} \\ &\approx \frac{1}{7.919} \\ &\approx 0.1262 \end{aligned}$$

Thus, the probability of reporting when *Confidence* is 0 is approximately $P(y = 1) \approx 0.1262$ or 12.62%. Hence, we can say our hypothesis is valid and that the confidence in women's ability to handle cyber-attacks significantly correlates with reporting cyberbullying incidents in this case. Table 5.20 shows the classification report for university students.

Class	Precision	Recall	F1-score	Support
0.0	0.65	1.00	0.79	65
1.0	0.00	0.00	0.00	35
Accuracy			0.65	100
Macro avg	0.33	0.50	0.39	100
Weighted avg	0.42	0.65	0.51	100

Table 5.20: Classification report

Secondly, we test Hypothesis 2 for University students.

The result of the logistic regression by the model:
Coefficient (Impact of Confidence): [[0.09883362]] Intercept: [-0.84612252]
The coefficient of confidence is 0.09883362 which is positive; it indicates with increase of confidence, likelihood of reporting of cyberbullying incidents would increase. The Y-intercept represents when confidence=0, as the intercept is negative, the probability of success would be low.
Then we calculate the probability of reporting when *Confidence* is high, using the logistic function:
Where:

- $\beta_0 = -0.84612252$ (Intercept)
- $\beta_1 = 0.09883362$ (Coefficient for Confidence)
- Confidence = 5 (High Confidence Level on Likert scale)

First, we compute $P(y = 1)$ when the confidence is high (i.e., Confidence = 5):

$$\begin{aligned} P(y=1) &= \frac{1}{1+e^{-(-0.84612252+0.09883362\times 5)}} \\ &= \frac{1}{1+e^{-(0.64804558)}} \\ &\approx \frac{1}{1+0.5231} \\ &\approx \frac{1}{1.5231} \\ &\approx 0.6565 \end{aligned}$$

Thus, the probability of reporting when *Confidence* is high (at a value of 5) is approximately:

$$P(y = 1) \approx 0.6565 \quad \text{or} \quad 65.65\%.$$

Now, we compute $P(y = 1)$ when the confidence is 0:
Where:

- $\beta_0 = -0.84612252$ (Intercept)
- $\beta_1 = 0.09883362$ (Coefficient for Confidence)
- Confidence = 0

Therefore:

$$\begin{aligned} P(y=1) &= \frac{1}{1+e^{-(-0.84612252+0.09883362\times 0)}} \\ &= \frac{1}{1+e^{-(-0.84612252)}} \\ &\approx \frac{1}{1+2.3305} \\ &\approx \frac{1}{3.3305} \\ &\approx 0.3002 \end{aligned}$$

Thus, the probability of reporting when *Confidence* is 0 is approximately:

$$P(y=1) \approx 0.3002 \quad \text{or} \quad 30.02\%.$$

Hence, we can say our hypothesis is valid and that the confidence in women's ability to handle cyber-attacks significantly correlates with reporting cyberbullying incidents in this case.

Lastly, we test Hypothesis 2 for Working women.

Class	**Precision**	**Recall**	**F1-score**	**Support**
0	0.71	0.96	0.81	23
1	0.50	0.10	0.17	10
Accuracy			0.70	33
Macro avg	0.60	0.53	0.49	33
Weighted avg	0.65	0.70	0.62	33

Table 5.21: Classification report

The result of the Logistic Regression by the model:
Coefficient (Impact of Confidence): [[0.37520137]] Intercept: [-1.72047116]
The coefficient of confidence is 0.37520137 which is positive; it indicates with increase of confidence, likelihood of incident reporting of cyberbullying would increase. The Y-intercept represents when confidence=0, as the intercept is negative, the probability of success would be low. Table 5.21 shows the classification report for university students.
Then we calculate the probability of reporting when *Confidence* is high, using the logistic function:
Where:

- $\beta_0 = -1.72104$ (Intercept)
- $\beta_1 = 0.3752$ (Coefficient for Confidence)
- Confidence = 5 (High Confidence Level in Likert scale)

$$P(y=1) = \frac{1}{1+e^{-(-1.72104+0.3752\times 5)}}$$

$$= \frac{1}{1+e^{-(0.15496)}}$$
$$\approx \frac{1}{1+0.8564}$$
$$\approx \frac{1}{1.8564}$$
$$\approx 0.5386$$

Thus, the probability of reporting when *Confidence* is high (at a value of 5) is approximately $P(y=1) \approx 0.5386 \quad$ or $\quad 53.86\%$
As opposed to when confidence is 0

$$P(y=1) = \frac{1}{1+e^{-(\beta_0+\beta_1\times \text{Confidence})}} \tag{5.3}$$

Where:

- $\beta_0 = -1.72104$ (Intercept)
- $\beta_1 = 0.3752$ (Coefficient for Confidence)
- Confidence $= 0$

therefore:

$$P(y=1) = \frac{1}{1+e^{-(-1.72104+0.3752\times 0)}}$$
$$= \frac{1}{1+e^{-(-1.72104)}}$$
$$\approx \frac{1}{1+5.590}$$
$$\approx \frac{1}{6.590}$$
$$\approx 0.17888$$

Thus, the probability of reporting when *Confidence* is low (at a value of 0) is approximately $P(y=1) \approx 0.1788 \quad$ or $\quad 17.88\%$

Hence, we can say our hypothesis is valid and that the confidence in women's ability to handle cyber-attacks significantly correlates with reporting cyberbullying incidents in this case.

5.6 Malware Detection

In the Malware detection sector, we have set four questionnaires. The answers that participants respond has given us a result of their malware manage and detection awareness. Moreover, it helps to assess their habit of safe downloading and recognizing malware symptoms. The responses are also mapped with a score of min 1 to max 4, where lower scales portray less awareness or bad practice and higher scores show strong awareness or good practice of cyber security.

5.6.1 High School Student

At first students were asked about how they would identify in case their device got infected. In the response of this question 42.8% students reported that they have no idea of how to detect malware. 21.5% responded that they identify through unauthorized activities indicator, while 35.2% students reported that they are not sure with the symptoms of malware.
Secondly, we analyzed students' cautious level while downloading any resources such as papers/games/movies from unknown sources and the result showed a mean value of 2.74 and st.dev. of 1.04 which shows that participants on average have a moderate to good awareness about being cautious while downloading resources from unknown knowledge.
Moreover, We analyzed the students' experience with malware detection tools. It shows a very low mean score = 1.67 and st.dev. = 0.80. Among all participants(n=395) 51.9% students reported that they have no experience in using malware detection tools. Only (n=16) 2.1% of students consider themselves as an expert in using malware detection tools. This low mean score indicates that the majority of the students has no experience of using malware detection tools and have less habit about cyber security practices. Lastly, When asking about how frequently they use anti-malware software, a result shows low mean score = 1.82 and st.dev. = 0.87. A majority of students (n=323) 42.4% never used anti-malware software, 22.1% infrequent users and only 4.6% (n=35) always use the anti-malware software to protect their device. This low score of using the anti-malware software indicates a significant gap in cybersecurity awareness and practice.

5.6.2 University Student

In the question of whether they can detect malware, the result shows that 45.3% participants response that they can identify malware by indicating the pop-ups, crashes and unauthorized access, 36.0% answers that they have heard about malware but unsure of the symptoms and 17.7% reported that they have no idea how to detect malware on device. To analyze the cautious level of downloading resources like academic papers, games, movies, we got a mean score = 2.89 and st.dev. = 0.88. This result indicates that participants are slightly more cautious than being not cautious at all. A mean score = 2.06 and st.dev. = 0.91 shows the answer of having experience in malware detection tools. 31.23% participants responded that they have no experience of using it and 5.41% participants reported that they are expert in using malware detection tools. Then again, asking how frequently they use it we got a mean score = 2.12 and st.dev. = 0.91 on answers, where 26.13% responded that they do not use it frequently and 5.71% participants reported that they always use it. The overall results show a low cyber security awareness and practice on malware detection.

5.6.3 Working Women

To assess the question of identifying malware, the result shows that about 51.% participants respond that they have no idea, 24.1% participants respond that they have heard about malware but are unsure of the symptoms. 24.1% participant response that they identify by malware indications. In the case of cautiousness of resource

downloading, we got a mean score = 2.58, st.dev. = 1.11. This result shows that working women have a moderate but insufficient awareness level. In the question of their experience of using malware detection tools, a mean score = 1.70, st.dev. = 0.91 shows the answer. About 54.62% participants shared that they have no experience and only 2.77% said that they are experts in using malware detection tools. Figure 5.5 shows the experience in malware detection tool result. A mean score of = 1.80 and st.dev. = 0.88 has shown on the answer of how frequently they use anti-malware software. About 45.35% participants responded that they never use it and 4.62% participants reported that they frequently use it. These results indicate that working women do not have a strong practice of malware and less awareness about malware.

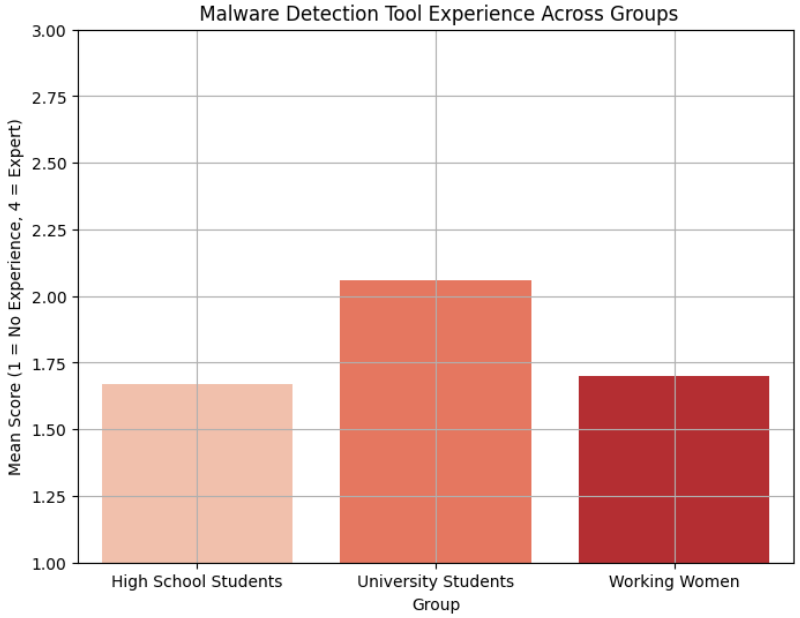

Figure 5.5: Experience in using malware detection tool (all three group)

5.6.4 Hypothesis 3: Testing

H3: Women's field of study and employment correlates with their ability to identify phishing examples and malware detection on their device.
For the analysis of this hypothesis the relevant questions:

- How would you identify the area your employment?/ How would you identify your field of study?
- Do you know "Phishing"?
- Which one do you think is an example of phishing?
- How frequently do you use anti-malware software to scan or protect your devices?
- How would you know if your device is infected by malware?

For the sake of convenience, we have renamed the following questions in a word according for easier data processing.

- 1. How would you identify the area of your employment? as **Employ**/ How would you identify your field of study? as **Studyfield**
- 2. Do you know "Phishing"? as **KnowPhlish**
- 3. Which one do you think is an example of phishing? as **PhlishIde**
- 4. How frequently do you use anti-malware software to scan or protect your devices? as **Malscan**
- 5. How would you know if your device is infected by malware? as **KnowMal**

We are using multilevel logistic regression's heat map to show the correlation of the factors between Studyfield/Employ against KnowPhlish, PhlishIde, KnowMal and Malscan. The map indicates the correlation between each corresponding factors assigning values to corresponding combinations. Value 1 indicates strong correlation while 0 indicates no correlation.

Firstly, we test the Hypothesis 3 for High school students

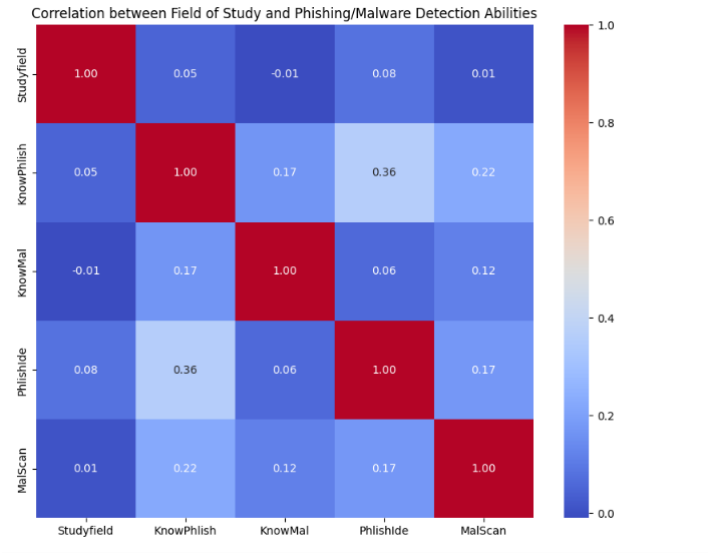

Figure 5.6: Result of Hypothesis 3 for high school student

For the above values from the Figure 5.6, we can see the correlation of studyfield with other variables, such as KnowPhish (0.05), KnowMal (-0.01), and PhilshIde (0.08) and Malscan (0.01) respectively. The correlation between the factors and studyfield can be considered negligible hence our hypothesis is invalid in this case.

Secondly, we test the Hypothesis 3 for University student

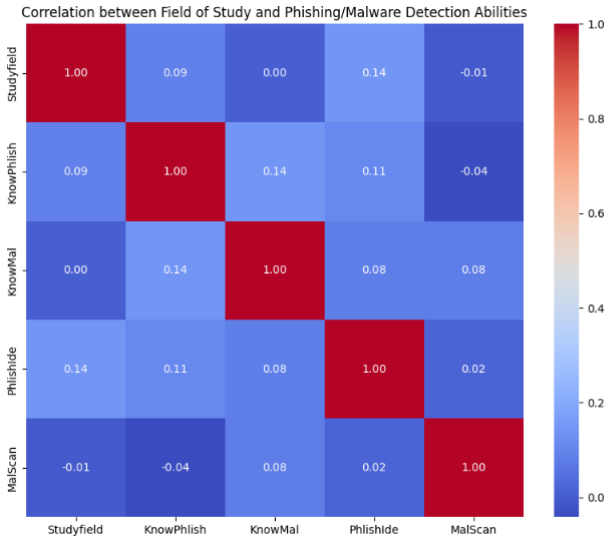

Figure 5.7: Result of Hypothesis 3 for university student

For the above values from the Figure 5.7, we can see the correlation of Studyfield with other variables, such as KnowPhish (0.09), KnowMal (0), PhilshIde (0.14) and Malscan (-0.01) respectively. The correlation between the factors and Studyfield can be considered negligible hence our hypothesis is invalid in this case.

Lastly, we test the Hypothesis for Working Women

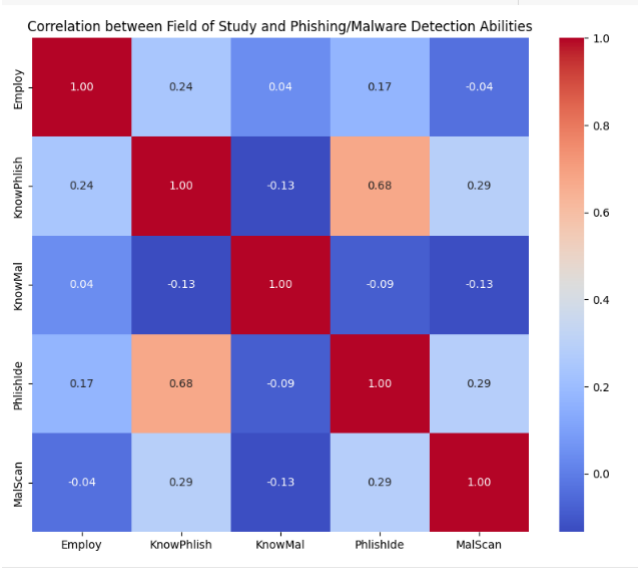

Figure 5.8: Result of Hypothesis 3 for working women

For the above values from the Figure 5.8, we can see the correlation of Employ with other variables, such as KnowPhish (0.24), KnowMal (0.04), and PhilshIde (0.17) and Malscan (-0.04) respectively. The correlation between the factors and Employ can be considered negligible hence our hypothesis is invalid in this case.

5.7 Insight from Paper Survey

Our data collection process was a combination of taking google from response and paper survey method. In the process of collecting data from the participants, we faced some inquiries from them. Almost every inquiry and asking we got was from the high school students. For the high school, we have used both of the methods of survey data collection but most of them participated through the paper survey method. In this method, we collected the data and had a face to face interaction with the participants. The students of 6th and 7th grade in rural area, actively uses digital devices and internet but they were very much unfamiliar with digital security practices. They student convey very hard time understanding the initial security questions that we had. Even though the questions were set in both bengali and english language for the better understanding, students were challenged by some technical questions. In the beginning of each of the factors of our question set, we gave a short description about it. For the students of 8th to 12th grade, they faced a hard time on understanding and answering the questions on phishing, two-factor authentication(2FA) and malware detection. Moreover, in the factor "Password security", apart from the given options we got some other unique response, such as a participant reported that she takes a screenshot of the password and keeps it in a hidden folder. Another participant responded that, she puts a note of the password's screenshot as a pin message in Viber (A communication platform). Finally, the survey used both online and paper-based questionnaires for the data collection and aimed at including different age and education level participants in order to represent the population. Some of the other students indeed shared non-traditional ways of securing passwords, for example some of them saved screenshots of passwords, which indicated potential flaws in their security behavior. Also a women share her experience, while she reported cyber bullying incident after many years which was more like a cyber harassement. The collected information can reveal detailed information about participants' level of cybersecurity knowledge, which can be useful in organizing educational campaigns for people of various ages in different environments.

5.8 Findings from Participants Comments

In our survey questions, there was an open ended question for any additional comments on cyber security awareness knowledge. There we tried to gather the person's expressed opinions without being limited to answering yes or no. From our large number of participants, we got some very constructive feedback, suggestions and insights which will help us while designing a framework. From the high school students, there were some comments. The answers reflect people's concern that gets more urgent when talking about cybersecurity issues or its absence, especially among precarious audiences like youth. Several participants pointed at the need of raising awareness of cyber threats; several participants focused on cyberbullying threats. It is also foreseen that parents should pay more attention and be knowledgeable about cyber security to be able to control children's use of the internet. Measures stating the prohibition of visiting suspicious links, protecting passwords and refraining from providing excessive personal data were mentioned as the most basic preventive measures. Further, there is a desire from the participants to have more seminars

to enhance security in the use of computers and the internet since these facilities are offered extensively in learning institutions. Some respondents stated they got enough information to satisfy themselves. In totality, the finding reveals an understanding of the need to have an enhanced education and awareness in order to meet the cybersecurity challenges.
The following responses from university students show an increasing awareness of the threat posed by cyber-criminality and of the lack of adequate safeguards in Bangladesh. Some students shared this opinion stating that cybersecurity should become an integral part of people's curriculum so that individuals are ready for digital dangers they can confront. Respondents also concurred there was a need for laws to be more rigorous so as to discourage cyber criminals. According to them, one should not access the sites of ill repute and should thoroughly avoid opening links in messages from unknown persons. Shifting to public Wi-Fi or if you are using your device with other people it is better to step up your security game and avoid possible attacks. Some focused on the methods of increasing the clients' awareness, since most of them have no idea how much of their information is available online. There were also concerns with special reference to the social media sites due to dissatisfaction with the existing complaints process regarding undesirable contents. The audience of students expressed a desire for additional practical workshops and information campaigns dedicated to prevention and measures to protect against cyber threats. All the answers suggest that people want to have more education, improved security for personal data and better tools to protect themselves.

Comments of the working women support the idea of rising awareness, cyber security is now crucial aspect of their lives and work, however, there is a clear absence of experience. Most participants demonstrated at least some aspects of basic security literacy, although this was more nuanced: for example, they acknowledged that one should not click on links from unknown people, knew that there should be a secret password, and understood that information is personal. Overall, there was a call for more knowledge and training. A few respondents outlined the overall awareness programs but references indicated that the company needs to reintroduce a stronger focus on incident reporting and the update of the software among all members. Some professionals are very thankful for broader efforts by certain organizations to raise awareness about some dangers of having an untrained workforce and open Internet addresses for any terrorist to access. In general, the working profession knows the significance of cybersecurity; the responses in the survey reveal the necessity to disseminate information further to increase awareness among employees.

Indeed, high school students, university students, and working women's feedback demonstrates the need to increase cybersecurity literacy. Even with such simple measures which include refraining from opening phishing links and protecting ones data there is great lack of knowledge especially when it comes to modern topics such as malware and cybercrimes. Regarding our propositions, all groups had an interest in increase in the number of seminars, workshops and tougher laws against cyber threats. These concerns creates a urgent need to advance targeted solutions to address the concerns and improve cybersecurity awareness for all.

Chapter 6

Interview Design: Development and Distribution

This chapter includes the design of qualitative study that has been conducted to identify and analyze the human behaviour and situational factors that influence women to engage in risky cyber decisions. To have more in-depth analysis on survey results we conducted our interview. As well, by conducting interview, we aim to identify all the potential risks and threats faced by women due to insufficient cyber security awareness. We undertook semi-structured interviews to analyze in a depth examining of cyber security knowledge, behaviour and situational factors. Through semi-structured interviews we understand women's knowledge about cyber security and how their cybersecurity knowledge affects their privacy and security concerns. This interview format is chosen to delve deeply into women's, behavioural patterns, perceptions and decision making processes in their day to day life activity. Through these interviews, We uncovered valuable insights into women's perception, action and their response to various cybersecurity challenges.

6.1 Purpose of Semi-Structure Interview

We have conducted a semi-structure interview for our qualitative analysis. A semi-structured interview often includes mainly open ended questions with follow-up probe questions for the interviewer to refer to throughout the interview [72]. For having a deeper understanding of the survey results, we conducted interviews for our further analysis. In our research, the interview questions cover a wide range of topics, from demographics and cybersecurity awareness to risky experiences and privacy concerns. A semi-structured format ensures these topics are addressed systematically while allowing participants to elaborate and bring up additional insights. Moreover, to analyze the background situational factor to any incident, we asked probing questions to get the depth of it. Our questionnaire is structured in six categories but different responses to different questions lead us to ask more of new questions. The response to the probing questions gave us more important data to our research. Thus, the interview session is conducted in a semi structured way.

6.2 Interview Sampling Method

In our study, we have adopted two sampling methods to choose our interview participants. Our prior importance was to choose the participants who were the best fit for the research. A standard interview sample requires 20 individuals to be involved in a meeting or discussion [3]. However, we expanded the sample size and conducted interviews with 30 participants to gain deeper insights and more comprehensive details. This larger sample allows us for a broader range of perspectives and enriched data while maintaining the depth of individual interviews. For sampling we followed, stratified sampling method [5], where the population was divided based on their three different demographics and snowball sampling method [1], where some of our participants referred us to other participants who met our criteria. These sampling approaches ensured that participants possessed the knowledge and experience necessary to provide meaningful insights into the research topic. The age range of the interviewee is from 12 and above, has encountered cybersecurity issues or privacy related incidents and has access and familiarity with online platforms where privacy concerns may arise. Participants were recruited through the email of google form that was collected from our survey, institutional networks and through some family networks along with ensuring the diversity in demographics. It was a 3 month process where we incorporated with the participants. We also cross checked their background to ensure the comprehensive range of perspectives. We used data saturation principles [75] to guide the sample size, where we conducted interviews until no new themes or meaningful insights were identified. This resulted in a study population of 30 participants. The combination of the semi-structured approach and the focus group setting allowed for rich data to be collected, consistent with the exploratory nature of the research.

6.3 Interview Participants

In our study we conducted interviews among our three participant groups: working women, university students and high school students. Figure 6.1 shows, the distribution of interview participants. There are a total of 30 participants. The university students hold the highest number of respondents with sample size of (n=16), then high school students (n=7), working women (n=7). All the participants are given an ID for the convenience to refer to them in the paper. The high school students with ID: HS, university students with ID: US and working women with ID: W. All the participants are literate people ranging from school students to professionals in workplace. The age range covered in the interview is 13 years to 35. From urban to semi urban areas of different divisions of Bangladesh this interview process highlights different experiences and perspectives of women. There are varieties of occupational and economic background among the respondents. Table 6.1 shows the demographic and device usage experience of all participants.

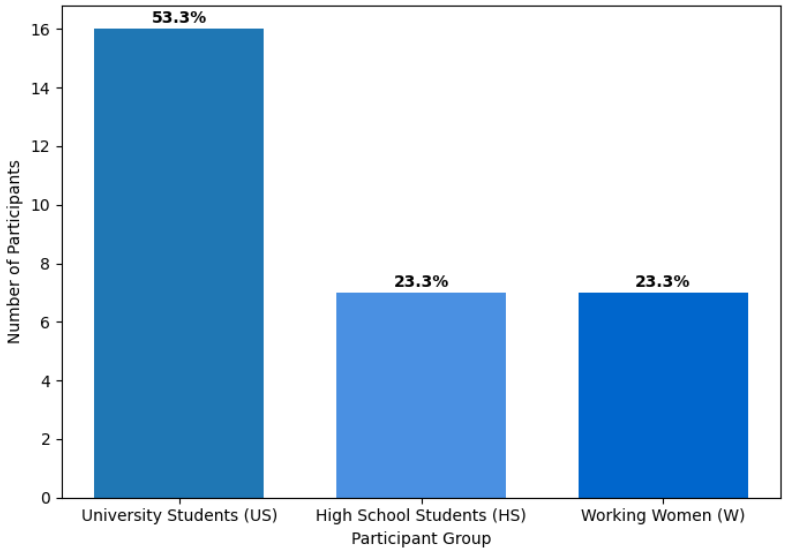

Figure 6.1: Distribution of interview participants

6.4 Interview Questions

To accommodate the three participant groups, we framed the same interview protocol differently to account for the three different perspectives. In this section we describe the interview flow. The interview protocol consists of six parts. The first part focuses on the participants Demographic information (age, academic/job status, economic status, resident area and years of using digital devices). The second part focuses on participants' basic knowledge on cyber security. We ask about what they understand about the term of cybersecurity awareness and also ask from where they have learned about it. Then we ask about their usage in digital devices such as participants' daily hour in using devices and for what purpose they use those devices. Moreover, their views on whether they think their activity in online is always safe or not were also asked. In the last section, we ask participants whether they have a personal device or shared device. In the third section, the questions were about if they have encountered any security threats and risky experience. Furthermore, we ask about the background reasons behind the negative experience such as what led them to take those decisions and what was lacking in their capability. Participants were also asked about reaction to those negative incidents for example, whether they took any action after the incident or ignore it. In the response of taking action we asked them specifically about the method. We also asked them how they have planned to handle the negative situations in future if that happens again. The next question was about their inspection on the mostly targeted online threats to women. This section concludes with asking participants whether their social account ever got hacked or noticed any suspicious activity and what they think is the main reason behind it. The fourth section was about privacy and security concerns of the participants. In this section, at first, participants were asked what they think about digital privacy and security. Secondly, we asked them, to what extent they share their personal information and whether they feel safe and secure to share personal information online. Moreover, participants were asked about which privacy and security features of any websites or apps are mostly trustworthy and not trustworthy to them. At last, in the suggestion and goal section, the questions

Group	ID	Age	Background	Area	Device Exp.	Hours/Day
High School	HS1	13	Class 6	Urban	4 years	4-6
	HS2	15	Class 10	Semi Urban	5 years	1-1.5
	HS3	15	Class 10	Urban	5 years	5-6
	HS4	20	Class 12	Urban	5 years	17
	HS5	15	Class 9	Urban	4 years	3-6
	HS6	20	Class 11	Urban	3 years	8-9
	HS7	14	Class 8	Semi Urban	4-5 years	1-2
University	US1	21	BBA	Urban	10 years	4-5
	US2	23	EEE	Semi Urban	10 years	6-7
	US3	21	EEE	Urban	8 years	3-4
	US4	24	CSE	Urban	8-9 years	5-8
	US5	23	BBA	Urban	7-8 years	3-4
	US6	23	Chemistry	Urban	7-8 years	6-7
	US7	23	EEE	Urban	10 years	4-5
	US8	23	Bioinformatics	Urban	7-8 years	7
	US9	23	CSE	Urban	5 years	10
	US10	23	CSE	Urban	5 years	9-10
	US11	23	Biotechnology	Urban	4-5 years	1-2
	US12	23	Microbiology	Semi Urban	10 years	10
	US13	20	EEE	Urban	10-11 years	9-10
	US14	24	CSE	Urban	15 years	6-8
	US15	19	English	Semi Urban	10-12 years	4
	US16	23	EEE	Urban	7-8 years	10-14
Working Women	W1	26	Banking	Urban	10 years	4
	W2	25	IT	Urban	8-9 years	4-5
	W3	26	Business	Urban	10 years	12
	W4	32	Admin	Urban	12-13 years	15
	W5	35	Textile	Urban	10 years	7
	W6	33	Tele Marketing	Urban	10 years	12-16
	W7	28	Business	Urban	4-5 years	3-4

Table 6.1: Demographics and Device usage by groups

were about asking suggestions for other women. Furthermore, participant's advice on educational resources or training were also asked. In addition, a question was asked about cybersecurity policies, features or improvement participant's want to feel more safer while browsing the internet. At the end of the interview session, we took suggestions about what kind of learning and essential resources would be enough to improve cybersecurity understanding.

6.5 Ethical Consideration

Ethical considerations are a crucial part of this study to ensure participants' rights, privacy, and well-being are safeguarded throughout the research process. In our interview process, all the participants were provided with a detailed interview consent form, outlining the purpose of the research, it's method and their voluntary involvement. For the school students, the oral consent from their parents is also

taken. The consent form describes that participation is entirely optional, with the right to withdraw at any time without any repercussions. To address privacy concerns, the interviews are audio-recorded with explicit consent and participants can choose to skip any question that causes discomfort. Anonymity and confidentiality are guaranteed and all the data are securely stored and used solely for research purposes.

6.6 Interview Conduction

Interviews are initiated by building rapport and reiterating the research purpose while also confirming permission to record. The average interview time is 20 minutes 13 seconds. The interview has been audio recorded with the consent of the interviewee and while taking interview, interviewers took notes of the important key points. The interview conduction process for this research is designed to ensure a seamless, ethical and insightful experience. All the Participants are provided with flexible scheduling options for either in-person or online interviews. The in-person interviews were mostly done in cafes, restaurant and institutional premises and participants' residences or offices. The online interviews are done in video calls through google meet. Prior to the interview, participants received a consent form outlining the study's purpose, methods and their rights which includes the freedom to withdraw at any point. The semi-structured format allows the interviewer to follow a guide while encouraging participants to elaborate on key topics such as cybersecurity awareness, risky experiences and privacy concerns. Sensitive topics are approached very patiently and probing questions are used to gain deeper insights. Finally, participants were thanked and compensated with the utmost amount of BDT 500 TK for their time afterward. In order to make use of the interview time more effectively and to refresh participants' memory with a risky privacy incident that they had recently experienced, we asked most of the participants to take a short pre-questionnaire one or two days or a week before the interview session took place. The questions mainly focused on the context of their reported privacy threat incident which later explored in details during the interview.

6.7 Interview Analysis

In this section, the methods used to analyse the interview data are described in detail. The analysis process involves categorizing and interpreting the data to extract meaningful insights. We employed an inductive approach [3], for thematic analysis and narrative analysis. Inductive analysis allows themes to emerge naturally from the data rather than being imposed on predefined categories [3].

6.7.1 Thematic Analysis

Thematic analysis is a method for identifying, analyzing and reporting patterns within qualitative data [99]. Thus, we used thematic analysis to identify the experiences and inherent themes from response. By using thematic analysis, we were able to uncover different knowledge levels and instinct of participants, which provides a structured understanding of participants' views. Initially all the recordings

were transcribed by the interviewer. Next, three interviewers repeatedly read the transcript to get a deep understanding. A shared codebook was proposed at the beginning which was iterated, finalized and reviewed in several meetings. We created our codebook based on the responses which expanded with additional codes that emerged through open-coding the transcripts. The final version of our codebook is in Appendix A.2. We used coding as a strategy to make sense of our data. The creation, coding and discussion of agreement and disagreements helped us to understand the data and formulate the themes that we describe in our findings.

6.7.2 Narrative Analysis

Narrative analysis is a method that focuses on the stories participants tell and how those stories are structured to make sense of their experiences [18]. Through narrative analysis this study focuses on how participants described their experience of risky incidents and their digital safety practices. This method helps understanding the individual perspectives, knowledge and emotions, providing a deeper understanding of how cybersecurity knowledge is influenced by personal experiences. To conduct this analysis, we transcribed all interviews' audio recording then carefully analysed each transcript to identify patterns like the main story of their online threat, their challenges, experience of learning and the change in their behaviour or practice. By reviewing iteratively, we identified recurring patterns, unique experiences, participant's reaction to the incident and pivotal factors in participants' awareness of digital security. Here we used an open ended codebook Appendix A.3 to identify key themes which were emerged from the participants.

The result of interview design is comprehensively discussed in Chapter 7 - Interview Findings: Addressing Vulnerabilities and Strengthing Resilience.

Chapter 7

Interview Findings: Addressing Vulnerabilities and Strengthening Resilience

This chapter presents the findings from the interviews conducted from our three groups of demographic. Exploring participants' cybersecurity awareness knowledge, device usage practice, security threat and risk experience, privacy and security concerns, suggestions and goals, this interview session reveals the potential risks and threats faced by women due to insufficient cyber security awareness and human behaviour and situational factors that influence users to engage in risky cyber decisions. This chapter is structured to demonstrate the detailed analysis of participants' experience, knowledge, perceptions and their call for change in digital policy and structural suggestions. The aim of our interview is to highlight the diversity of experience and response across high school students, university students and working women.

7.1 Risk and Threats Encounter by Participants

This section explores the risk and vulnerability that arise from user inadvertent and risky behavior and identifies the consequences that arrive from users' online interaction and activities, substantially privacy and security threats. Analyzing participants' understanding of digital privacy and security this section focuses on how women use the internet and their digital devices. Exploring the participants' response we got various kinds of security and privacy threats experienced by them that address the RQ2 of our research. To identify the risk and threat encountered by the participant, we constructed code for patterning threats. Figure 7.1 shows the distribution of emerged threats of the reported stories. The participants expressed their faced risky situation through a story which later, through analysis is deduced to identify the reported threat.

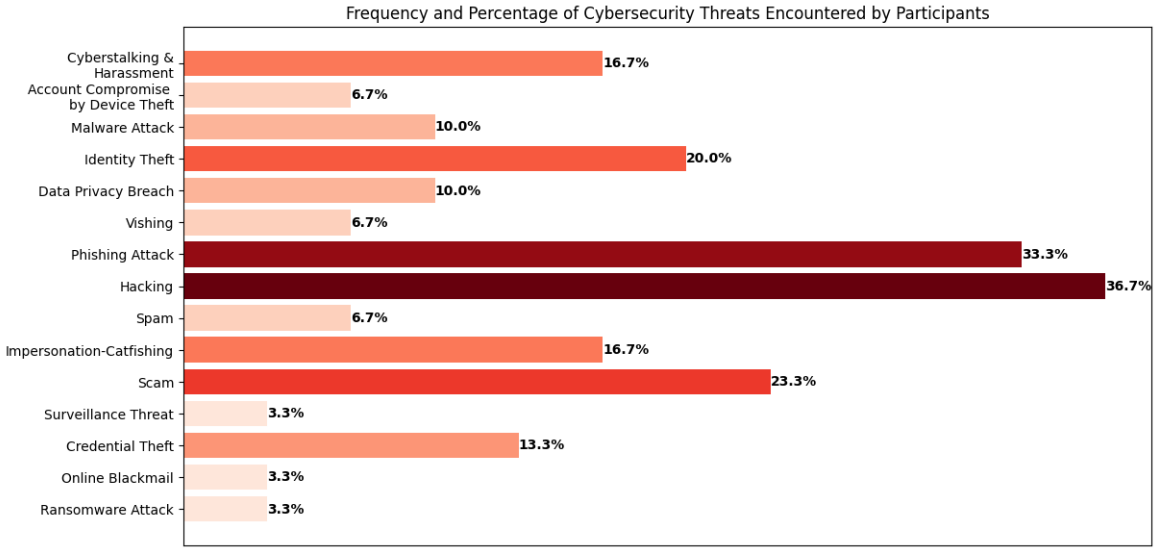

Figure 7.1: Cyber security threats encounter by paricipants

7.1.1 Cyber Security Awareness Knowledge

From our interviewee, initially we have underscored the cybersecurity awareness knowledge that participants have. Many participants showed a good understanding whereas few participants had no insight on cyber security awareness at all. Some of the participants provide actionable examples like securing Wi-Fi, not logging into unknown devices and managing information after logout is cybersecurity awareness to them.

> *"When we are using internet we need to maintain some precautions like the wi-fi I am using is secure or not, am I logging in to others unknown devices and not deleting my information when I am logged out or not etc,. Basically these are the things I do understand about Cybersecurity Awareness."* - HS2

The participants also shared that their activity on their device or internet is always safe to them, most of the responses expressed out negatively. Very few of them considered it to be safe as they claim to use their own device and not share their passwords with others. The interviewees also emphasizes privacy, data safety and awareness about information leakage by revealing critical cybersecurity concerns along with focusing on protecting personal information, especially on social platforms. In the meantime, some of them oversimplify cybersecurity and have vague ideas about it. About the understanding of cybersecurity awareness knowledge, some of them provided only a basic behavioral notion where a participant explicitly shared:

> *"I am not sure about it"* - US11

Participants are mostly worried about auto-saving their passwords in their account. The practice of ignoring security warnings also indicates that their practice toward the internet is not safe. The feeling of being monitored by their devices makes them unsafe as well. Moreover, some of the interviewees were not able to provide any cause if their device usage practice is safe or not.

"No, I do not feel safe because when I download a game, they ask for personal information and I give it. Later I realised, my activity was not secure." - HS1

7.1.2 Phishing Attack

Phishing is the act of attempting to pay off information such as username, password and credit card details as a trustworthy entity in an electronic communication [49]. A large portion about 33.33% of our participants shared stories about how they have become victims of phishing attacks. The majority of this attack were by deceptive links, phishing apps and website design to steal sensitive information via message and social media. As a result of the phishing attack, the participant has lost their social media account, data and also faced financial threats. The attacker impersonates a legitimate organization or individual participants into revealing information. HS6 expressed that how she became a victim of phishing attack.

"I downloaded an app from google play store named "View Insta Follower" to check who didn't follow me back on Instagram. In order to log into the app, I provided my Instagram login information. The app worked as expected, and I was able to see who had not followed me back. However, after using the app, I returned to my official Instagram account and I saw I had been logged out and was given to enter my login information again. Upon trying repeatedly, I found that my password had been changed. Fortunately, I was able to recover my account since it was linked to my Facebook profile."- HS6

Another participant highlighted that her facebook id has been hacked through a message, delivered with a link providing a free coupon for a restaurant. Moreover, several participants shared that their known person shared the link that redirects to phishing attacks. Most of the participants shared their personal account information and fell into the tricks.

"From my friends id I was given a facebook link where it said, if I like this page I will get an offer in parlour service. To like the page and claim that offer, I clicked on the link, which took me to a page resembling my facebook login screen, so I gave all my login info and then I found out that it was a movie website. After that I realized, I lost all access to my facebook and my account got hacked. Then the hacker used my personal information, and spread my private photo." - US7

7.1.3 Account and Identity Compromise

We found many generic stories on impersonation and catfishing faced by participants. About 16.67% of them faced this threat in their device and internet usage. The attack occurred in a way that participants compromised their identity, either partially or completely. Participants' incidents show how through impersonation they lost their sensitive data and got harm which often led to emotional stress and insecurity. Victim's reputations were often ruined. In some cases, it took them a long time to resolve the problem.

> *"I used to leave my phone at home when I went out and often felt like someone was using it. When I came back I used to see some of my messages being seen. One day I went out to a restaurant and saw some random boys there, which is not supposed to happen. As I used to share my room with 2 other girls. Then I checked my phone and saw a visiting history of those apps where I haven't visited for the last 2 days. Moreover, messages from my account were also sent to some boys such as where I go, someone informs them. Later I found out my roommates used to sneak in to my phone."* - HS4

Several participants also reported how fake identity creation was built to gain trust from other people. Participants revealed how after impersonation hackers request money from others and exploit their photo and data to unwanted sites.

> *"My facebook account got hacked and the hacker asked for money from my friends through my id saying that I am in a great need and urgently asked to send the money to me. Some of my friends gave the money and others later informed me about this incident.This experience was very much unexpected and heartbroken. I had to go through a lot of mental stress. After seeing all my messages, the hacker got a very deep understanding of how I talk and very smartly he did this."* - W1

Another respondent shared an unexpected incident where she lost her instagram account and that account was actively using her identity for months. Also, in expressing the incident face by US12 she shared,

> *"There were many facebook fake accounts on my name and from one of those accounts, it sent some inappropriate messages to my parents and to my friends which made me embarrassed in front of them."* - US12

In addition, 20% of participants reported incidents that align with identity theft. They narrated stories which include how their identities were stolen through hacking and phishing. Some stories report the usage of fraudulent websites or hacking as the source of identity theft, while most claim not to know why this happened.

> *"Someone took my photos from my account and created a fake account" Moreover, any report did not work as it got more followers than my real account."* - US8

HS7 shared how her account got compromised by device theft. She expressed,

> *"I use my mothers facebook id to be connected with my friends. One day my mother's phone got robbed and after some day, my mothers facebook account also got hacked and I think it was by the thief who robbed my mother's phone as I didn't use any device lock system in my phone."* - HS7

Similar to this, HS2 also experiences account compromise by device theft. Participant's whatsapp account got compromised by unauthorized access.

After all this, we found a case where participants encountered surveillance threat. It refers to unauthorized monitoring or tracking of an individual's activities particularly without their consent or knowledge. US6 shared an incident, where her device was located by locate-sharing features. While sharing story she expressing that,

> *"My abroad living husband tracks my location and this is very uncomfortable to me."* - US6

We found many stories of data breaches affecting leaking phone numbers to unauthorized access. Again some participants were not sure how their sensitive data were breached.

7.1.4 Malware & Ransomware Attack

Some of the participants shared stories related to virus or malware attacks. The victims' computers or phones or laptops were the medium of this attack. From those that described the viruses in more detail, that screens behaved differently, got frozen or turned blue or blink and devices slowed down or crashed. About 10% of participants are victims of malware and 3.33% of ransomware attacks.

> *"I downloaded a movie from a random illegal website using my father's laptop and then the laptop was attacked by virus and malicious software for which I lost many of my father's important files and photos."* - HS3

A story describes attacks that locked her computers and encrypted data, asked the victim to pay a ransom in order to regain data access. The reason described as the source of the ransomware is clicking on suspicious links. Moreover, the requested amount for data recovery was huge.

> *"In search of a movie subtitles, I randomly download a file from a very unknown source, after that all my files in laptop got locked, clicking in my files it was showing a message that "If you want to retrieve your data, then provide xx amount" also ask for my mail and gave a number. I couldn't understand what was that."* - US4

In that mentioned story, asking whether the ransom was paid or not, the participant shared with us that she could not provide that ransom and eventually lost all important files from her laptop.

7.1.5 Vishing

Vishing is a voice phishing attack, whereby a voice call received from an assailant lures the target into providing personal information with the intention to use that information to cause harm [38]. About 6.67% of participants are victims of vishing attacks. Vishing is designed for identity theft where user profile or access credentials are stolen. All of the cases from our obtained data refer to financial fraud.

> *"From my bkash account I lost 10k taka by a random call. The scammer called me pretending to be a bkash agent and asked me about my OTP and at that time I was new to bkash and they tricked me and I gave my OTP number to them. Then I immediately lost my account with 10k money."* - W6

Again, HS5 used her mother device and was not aware of scammer's ability to use techniques such as OTP sharing, providing device access, password privacy and advanced automated systems to commit this kind of fraudulent.

> *"Once one random caller said someone mistakenly deposited money into my mother's account thus my bkash account got locked, to unlock it he was giving me some command to follow in the phone I gave him my phone access and my OTP instantly. I was so afraid that I did not even check to see if my account was actually locked or not. After that he even asks if I have a bank account or not. After a while he cut the call and when I checked, I saw my account was not locked and 20K taka was transferred to an unknown source."* - HS5

7.1.6 Social Media Hacking

A majority of the participants shared stories that are about their social media hacking. 36.67% of them were hacked on facebook, instagram or whatsapp. This hacking mostly executes through phishing attacks, where others are reported to be hacked as they had no security feature activated on their device and one victim could not identify the reason behind the hacking. As a result of the hacked account various threats occurred such as sending spam messages to others, making transactions, stealing personal photos and personal identity exploitation.

> *"I do not know how my instagram account got hacked as I did not use my account for the last 5-6 months. After months when I tried to log into my account I was failed and later I discovered that my account had been active since the last time I stopped using it."* - W5

It is reported by the victims that, once an account is hacked, it often serves as a gateway for further exploitation such as identity theft, unauthorized data access and financial fraud.

> *"Once I randomly clicked on a link, which took me to a website but there was actually nothing. I did not give any attention to it and after sometime one of my friends called me saying that why I am posting all these unnecessary things (bitcoin numbers etc.) from my facebook account and then I tried to log into my account and was not able to log in. That was the moment I realised that my facebook account has been hacked."* - US10

A significant proportion of hacking incidents occurred through another hacked account. Participants were given links or messages from their friends on social media and lost their account.

> *"I got a random link from my known friend where it was showing an offer to obtain so that I gave all the informations it asked like my gmail, phone number and facebook password. After a while, a mail of unauthorized access on facebook came to me. Also, the location of the access was far away from me. Then I realized my account is hacked. my friend informed me that the link I had sent them led to their account also being hacked."* - US16

7.1.7 Spam and Scam

A range of participants potentially fell victim to a spam and scam. Spam and scam refers to unsolicited, irrelevant or repetitive messages sent via email or social media platform, in order to trap users into fraudulent schemes and harassment [27]. About 23.33% of users are a victim of spam and 6.67% of scam. The participants who encounter data breaches are often exposed with spam and scam.

> *"For the last 1.5 years, there has been a guy who calls me frequently at night from a Malaysian number at late night and I ignored it for a long time. One day, I finally picked up, and I got shocked that the caller knew my nickname and whereabouts. Then he suddenly started using slang words which scared me a lot. I still get a lot of unknown calls and unwanted messages where those person know every details of mine."* - US11

Other participants stated how through spam messages in their social media they got targeted to phishing, hacking and other privacy breaches. Another frequent concern is about scamming, where attackers pretend as representatives from authorised agencies, resembling legitimate sites, are used to extract personal data or money. Some participants shared incidents involving fraudulent job offers, fake websites which are designed to exploit credential details resulting in massive financial losses.

> *" For travelling I purchased a bus ticket from a ticket selling website which I randomly found on the internet. Then I paid through bkash. I provided almost 8000 TK but when I went to see if my ticket got booked or not as I did not get my e-ticket. Then I called the bus line service and they told me that those seat numbers are still available and they did not sell that ticket to me. They said several website use their bus line name to sell ticket which are not authentic"* - W4

Consistently, other participants fell victim to advance fee scams, where they paid upfront to a website but never received the product. US13 explained with grief that she had to pay twice to reclaim her order. Moreover, participants also shared about a scam where they fall into the cunning trap of offering prizes, gifts and easy ways of earning money. Therefore, those tempting offers led them to attack later. These incidents highlight how participants are exploited through scam and spam.

7.1.8 Cyberstalking Harassment and Online Blackmail

From our analyzed participant, about 16.6% of participants reported becoming the victim of cyberstalking harassment and online blackmail. Using social media or via any digital communication, harassing, monitoring or threatening someone is referred to as cyberstalking harassment [10]. From the findings of HS1 it reveals that cyberstalking causes fear and emotional distress to her.

> *"I use snapchat for taking photos and communicating with my friends. Unconsciously I clicked on the add option and one random elderly man got added into my snapchat account. He saw my photos and texted me saying that knows my home address and the address he said was correct.*

He threatened me that he would come to my home and take me. I got scared and deleted my account. Later I realised my location was keep on in snapchat." - HS1

In addition, participants also shared that they get inappropriate pictures and hatred messages on their social media account. Despite the cyberstalking incident, participants also shared about how they became victims of online blackmail. Through online blackmail, the blackmailer threatens, extorts someone by using individuals' sensitive and personal information and manipulates or controls the victim [73]. US7 shared her story of getting blackmail by an unknown person on social media. To express her incident she shared,

"Once my facebook account got hacked and then the hacker used my personal information, and spread my private photos. Through another id, I tried to reach the hacker then he was asking for money and blackmailing me, by saying, if I give him a private photo of me, he will give back my id." - US7

Finally, from this section we obtained key findings on what risks and threats are faced by women due to their cyber security awareness knowledge. A deep understanding of most prevalent vulnerabilities that affect women adversely in digital spaces. The findings emphasize on delving into these risks and threats and demand for a proactive approach to mitigate these challenges.

7.2 Behavioural Choices in Online Security: Causes and Responses

In this section, we meet our RQ3 through analyzing into the behavioural and situational factors influencing participants to take risk in digital landscape, exploring the reasons behind engaging in risky cyber decisions. Understanding these behavioral patterns provides insights into causes participants knowingly or unknowingly compromising their security. Morover, this section highlights the users response on online security and privacy concern warning. The section also analyzes how they react after encountering security threats, participants' action, inaction on their threats.

7.2.1 Human Behaviour and Situational Factors Influencing Risk Taking Decisions

Through an in-depth examination, we analyed human security behavioural patterns. Personality traits have largely been studied in the context of phishing susceptibility [51]. Therefore, we evaluate human behavioral and situational factors that influence them to take security and privacy risks. We categorized users' reported causes with eight key behavioral situational factors that directly indicate and contribute to the most commonly emerging cyber security risk. Figure 7.2 shows categorized human behaviour and situational factors that influence users to associate with risk and threats.

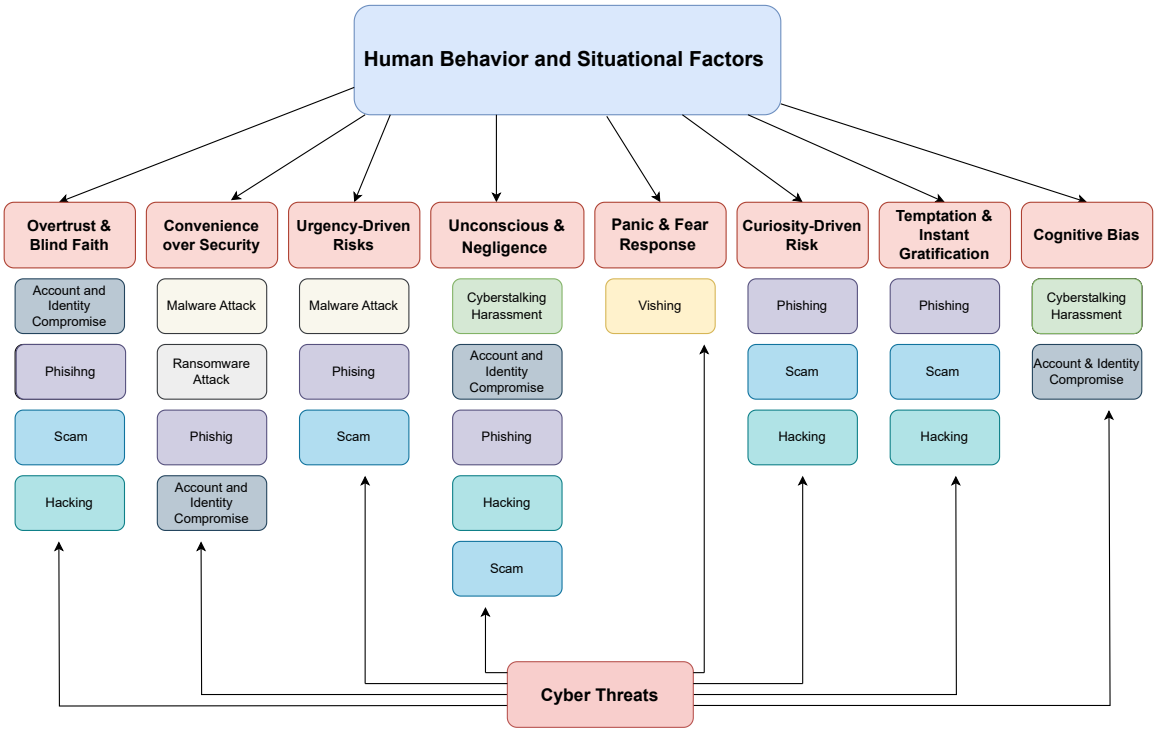

Figure 7.2: Human behaviour and situational factors that influence users to associate with risk and threats

Respondents characterized with cognitive bias mostly fall into cyberstalking harassment, account and identity compromised risk. Their overconfidence and belief to be less likely to fall for threats has adversely resulted here. Also, participants possessing temptation and instant gratification are predominantly vulnerable to phishing, hacking and scam. Their decision making tends to prioritize more on immediate rewards over security protection. Panic and fear response also influence participants to encounter with vishing. Creating an urgency and high-pressure, cybercriminals compel individuals to act impulsively and irrationally. Respondents exhibiting unconsciousness and negligence are more prone to be at higher risk of cyberstalking harassment, account and identity compromise, phishing, hacking and scam. Their tendency to overlook privacy and security settings mainly increase the susceptibility to cyber threats.

In addition, urgency-driven risk is frequently reported behaviour that also exposed to malware attack, phishing and scam. Their tendency to act on hastily and immediately overshadow the potential risk. Those who choose convenience over security are mostly susceptible to malware attack, ransomware attack, phishing and account identity compromise. They significantly chose their needs while bypassing essential security measures, prioritizing ease of access and immediate results over security precautions. Moreover, participants engaging in risky behavior displaying curiosity-driven risk also associate themselves with phishing, hacking and scam. Finally, overtrust and blind faith in digital interaction significantly cause account and identity compromise. This is also a cause for phishing, scam and hacking. These participants often fail to recognise the threats and questions the authenticity and

credibility of that offer request or message, which later emerged as threat.

7.2.2 Major Weaknesses Exposing Women's to Cyber Risks

In response to the lack and incapability that participants made a victim of risk and threats they shared various vulnerabilities and inefficiency that are mostly responsible for those. Insufficient security awareness, digital illiteracy, poor privacy control, weak security practices and inexperience with security features are mostly prevalent variables derived through our analysis. Figure 7.3 shows the underlying causes of cyber attack and data breach risks.

> *"The risk happened to me, because I did not know there is a feature about location. My location was always kept on. I never looked for security measures in my usage rather than using snapchat."*- HS1

As well as, HS4 encountered with account and identity compromise express the weak security practice that she has. Stating,

> *"The main reason for this threat would be not using any password or pattern lock in my device, I felt it was unnecessary and an extra hassle."* -HS4

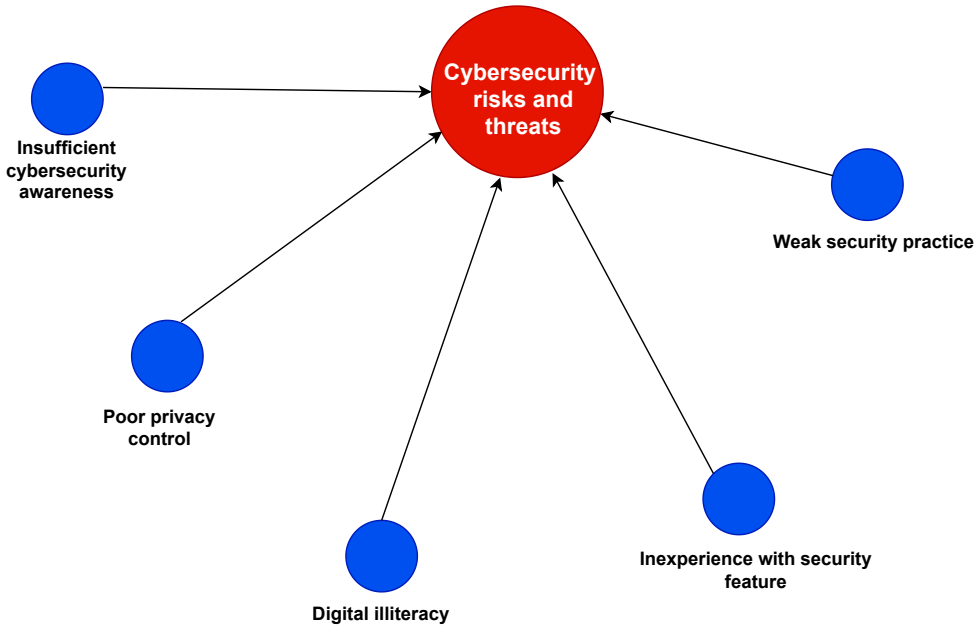

Figure 7.3: Underlying causes of cyber attack and data breach risks

While being a victim of vishing HS5 stated that having weak security practices and insufficient awareness knowledge was the main reason for which she faced risk.

> *"I shared my OTP with the scammer and when I shared that, I did not know that OTP is something that can not be shared. Later after this incident I saw on a TV advertisement about not sharing OTP with others ever. To be honest, I spent a good amount of time on social media but never saw a single post regarding this"* - HS4

A significant number of participants show poor privacy control as they never use two factor authentication and share personal and sensitive data to unverified and unknown platforms.

> *"I did not know how my social media account was hacked and someone else was using my account pretending to be me, If I used two factor authentication, I might have get a notification that someone is trying to break into my account"* - W5

Similar to this, many others reported that they shared too much personal information over their social media accounts and it was an impulsive decision to take on.
Furthermore, digital illiteracy drastically contributes to the exposure of risks. Participants often fail to use digital technologies, tools and resources effectively and confidently. H6, one of our participants downloaded an app which was designed to steal credential informations. This incident reflects a lack of understanding of the risks involved in using third-party apps. Similarly, W4 paid on fraudulent websites which again shows the lack of knowledge about verifying the authenticity of websites prior to making payments. Finally, a significant portion of participants explicitly stated that for having inadequate cybersecurity awareness knowledge, they mostly experience these risks and threats.

7.2.3 Women's Response to Security Warning

In the interview, we asked participants about situations when they saw an online security or privacy concern warning to understand what was their reaction, if they ignored the warning or took it seriously in their action. Among 30 participants, only 4 of them responded that they take security and privacy warnings seriously. Moreover, we asked if they ignored what were the reasons that pushed them to make those choices. Although in many cases, the participants mentioned more than one and the answers were transcribed and analysed. For each participant, the reason has been identified through thematic analysis. Here we have categorized four different rationales which are desensitization, dismissal of a pop-up, excessive dependency & trust in source. Figure 7.4 shows the categorised responses of users. The categories of rationale are identified as following:
Desensitisation: About 30.77% of participants reported desensitisation to warning as a reason for ignoring them. Participants are mostly habitually dismissed security warnings. Participants became accustomed to security warnings and started dismissing and ignoring them without even evaluating the upcoming risks. US5 explicitly stated that:

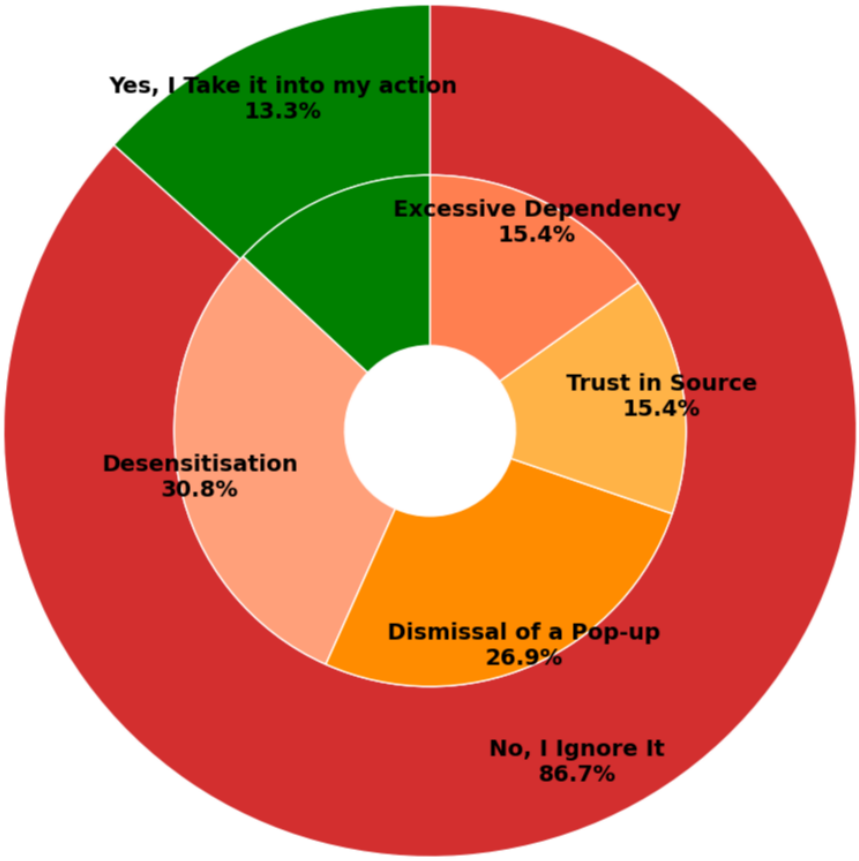

Figure 7.4: Users' response to security and privacy warnings

> *"While downloading a movie, I use some torrent websites. To allow the download, it shows some security warning, I thought the warning was just a routine thing, so I allow it because otherwise, they don't give me access. I mainly do it for urgency, academic need."* - US5

Similarly a lot of other participants also shared their repeated behaviour of dismissing the security warnings. Moreover, the extensive terms and conditions made them desensitized to security alerts. Also US10 shared with us that:

> *"Sometimes in a rush, I do not read the terms and conditions. I think it is a generic thing."* - US10

Dismissal of a Pop-up: Approximately 26.92% of participants indicated that they do not take pop-up warnings seriously because they found it annoying and for their urgency they mostly ignore it.

> *"Yes, I get pop up messages like warnings mainly while downloading or installing. For my urgency I ignore those messages."* - US6

US2 also stressed on why she dismissed the pop up warning. She shared,

> *"If I ever sign in with weak password I get a message that my password is not enough strong, but I actually do not take it seriously for my convenience."*- US2

Some participants also reported scenarios where they came up with warnings but they prioritized their needs more than security.

Excessive dependency: 15.38% of the participants revealed that due to their strong reliance on digital platforms, resource and service they overlook the security warnings. In favour of accessibility they make them vulnerable to cyber attacks.

> *"When I download any software, if that shows a warning, yet I download it because of my need. Also the crack version costs low. I do not prefer paying high. In this way even if I have risk I ignore it"* - US8

Also, the fear of missing out information led several participants to not respond to warnings or evaluate the warning message.

> *"I watch and download movies, dramas from pirated sites and that time I get warnings that the files I am downloading are not safe and contain harmful viruses. Still I use it as I am a student and can not effort Netflix, Amazon Prime or Hoststar."* - US15

Moreover, participants also reported that, for the need of academic help, they mostly depend on some specific resources, thinking only those can give them solutions.

Trust in Source: Finally 15.38% of participants' responses are categorized in trust in sources as they mostly disregard security warnings for being overtrusted to the source. Participants trust their friends, google play store and their cognitive bias that nothing negative may happen to them lead them to ignore the security warnings.

> *"Some apps that I download from google app store show me warning while using but mostly I ignore because I feel apps from google play store would be safe."* - HS6

Therefore, from our data, it shows that participants are making these choices in their behaviour and getting into attacks by ignoring the security warning even after having a partial knowledge of the consequences.

7.2.4 Action and Inaction

The bar chart in Figure 7.5 visualizes the action and inaction participants take when they encounter any cyber security threat. The chart reveals that the majority of respondents, about 33.33% did not take any action. They ignored it as they did not know what to do in response to that situation. Many individuals do not possess the necessary skills or resources to handle cyber threats immediately. We found 6.67% ignore reporting their faced incident because of the fear of their parents. HS2 shared that,

> *"I ignore the situation that someone has overtaken my whatsapp account and did not report anywhere and did not even share with my parents. I thought they would get angry with me and would take away my mobile phone."*- HS2

This fear among the younger individuals leaves them more vulnerable to repeated cyber attack. A substantial number of participants (23.33%) complain to the associate authority. However, among them some participants explicitly reported that they actually got no meaningful assistance, guidance or important information even after their report. Where 10% uninstalled or deleted their account as they found alternative methods lengthy and troublesome. Only 6.67% reported starting using two factor authentication in their account. Again 10% of participants reported seeking help from their friends.

Moreover, 6.67% went for a police complaint, revealing that some participants recognize the legal aspect of cybersecurity threats and 6.67% blocked the attacker in social media only if she could identify the attacker. Again, a small portion of respondents (3.33%) choose to take help from expertise. Emphasis on that professional assistance is rarely considered or accessible to the participants. The findings from this data shows various ranges of response to cybersecurity threats stretching from taking action to completely not taking any action.

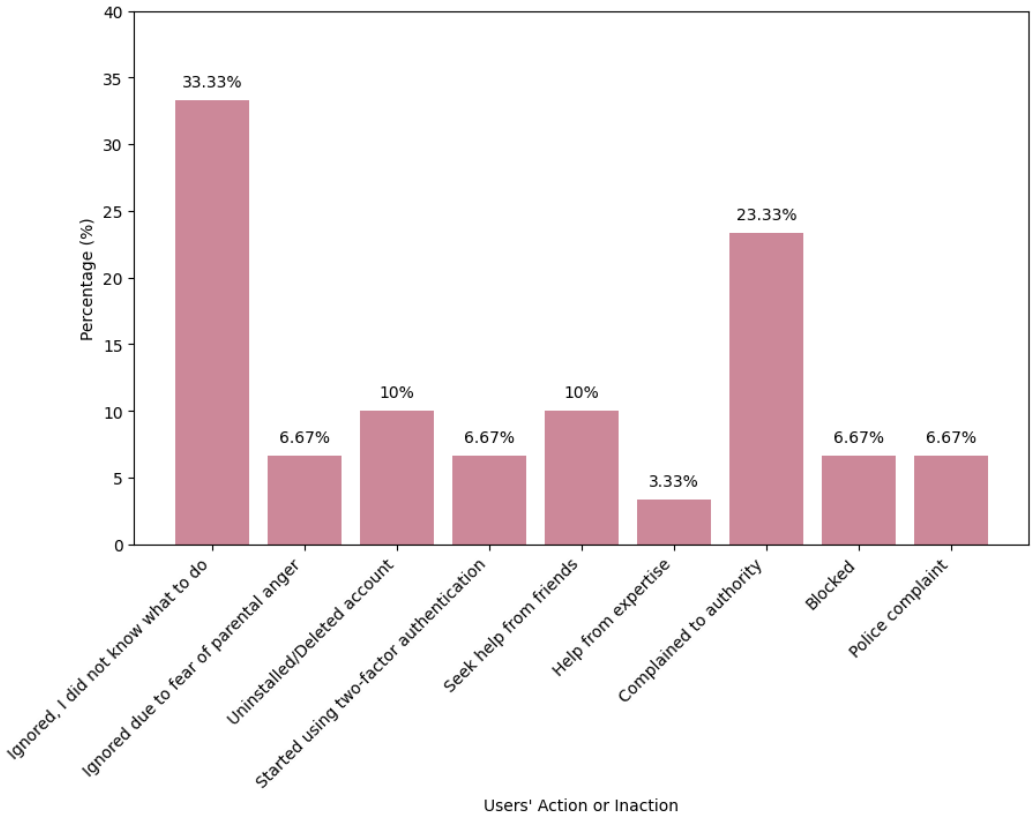

Figure 7.5: Users' action and inaction the the reported risk and threats

Finally, this findings of this section provides a comprehensive understanding of human behavioural, situational and underlying factors that influence users to engage in risky cyber decisions. The background reason of human behaviour and situational factors creates a relation with digital usage.

7.3 Women's Perspectives, Concerns, and Suggestions on Cybersecurity and Digital Privacy

This section explores women's experiences over security and privacy features, concerns and suggestions regarding cyber security, online threat and digital privacy. Analysing from participants' interviews, we inspected their preference for security and privacy features across various websites and applications that highlight user's reliability and concerns to that feature. Furthermore, their reported most targeted threat from women, suggestions on usage and awareness education. By analysing these, this section highlights women's collective voice in building a resilient cybersecurity knowledge and safe environment.

7.3.1 Women's Perspective on Security and Privacy Features & Policy

From our interview, we got a valuable and diverse range of opinion regarding privacy and security feature's preference and those features and an additional policy regarding improvement. Through analysis, we categorised trustworthy/safe and untrustworthy/unsafe features described by them. Table 7.1 demonstrate the participants views on trustworthy and untrustworthy security features in various apps and websites. One participant stated various features, were also later found common in another participant's opinion. As well as, we found some features where a participant marked it as untrustworthy but on the other hand, another participant tagged it as a trustworthy feature. Participants widely use social media. Therefore, the features they mentioned about are mostly related to social media apps. Participants emphasized on privacy safeguard features and two factor authentication features in facebook are trustworthy to them. Whereas, easily downloading photos from any facebook account without notification, unrestricted messaging, market place feature scam risk and facebook live features are less trustworthy and unsafe to them. Then a huge group of participants are instagram users where most trustworthy features to them are parental supervision, restricted messaging and instagram private mode feature. Then coming to untrustworthy and unsafe features they stated about follower visibility feature, profile picture accessibility and single sign on feature are most reported.

Furthermore, Participants who use snapchat stated that they found a trustworthy feature of snapchat where it sends notifications if anyone has taken a screenshot of a message or picture, also one participant liked the location sharing feature whereas others did not. Then an ephemeral communication system where messages automatically disappear from the recipient's side after viewing the message. From whatsapp, end to end encryption, contact only messaging, multiple login, qr code security is mostly trustworthy to the majority of participants. These whatsapp users speci-

fied that they do not find unrestricted contact based messaging and open group invitation at all in their whatsapp usage. Among all these, youtube is the most trustworthy and safe feature according to the participants, as it has limited personal information requirement, no direct messaging or contact based feature which makes it more convenient to use. Focusing on google features, google safety feature, password manager, strong password suggestion and find my phone are pointed out as the most trustworthy features. Again in gmail, false positives in spam filtering is reported as unlikeable. Participants also shared that they do not like password managers as it often leaks their credential information unknowingly. Imo is also reported as an unsafe app as it has unauthorized contact visibility and unrestricted messaging feature. Finally the find my phone in Apple and advertisement blocking feature in mozilla firefox is also reported as trustworthy and safe feature to the participants. This analysis highlighted the urgent need for this platform to address their security gaps.

Participants were also asked to provide their suggestions on policy and features for improvement. Significant participants convey that they want biometric authentication for a secure login in social media. Also they emphasize simplified terms and conditions, restricted account access and age verification systems improvement. They mostly stressed on security and privacy features improvement and changes where they mention that gap earlier. Through this in depth analysis on user preferences on security and privacy features and policy improvement we get valuable insight that needs to be addressed soon.

7.3.2 Women's Perspective on Online Threats Targeting Them

Our findings show that women get exposed to various kinds of risk and threats from their own experience. While collecting data from respondents, to express what specific online threats they think are mostly targeted to women, they shared a wide range of cybersecurity threats that affect women. The visualization in Figure 7.6 illustrates the emerging online threats that are mostly targeted in our country.

7.3.3 Women's Suggetions on Digital Usage & Privacy Protection

From all groups of participants, we got some key recommendations for a protective and safe digital environment. Various suggestions from three groups raised concern over ongoing cyber Security threats and challenges. Many participants feel that sharing too much personal information in social media and unauthorized sites can create potential misuse. The profile lock system in social media apps is also suggested as a way to restrict unauthorized access. To be protected and more careful on online US11 suggested that,

> *"We should post everything sincerely and make sure our profile lock. We also should not accept unknown people in social media"* - US11

US1 and US10 responses highlighted that enabling location tracking on apps such as social media can adversely affect cyberstalking. Participants also stressed on the importance of 2FA to secure ID and prevent hacking attempts. According to them,

Apps/Websites	Trustworthy	Untrustworthy
Facebook	Profile Shield Guard Two factor authentication	Public Photo Download Unrestricted Messaging Marketplace feature Facebook live
Instagram	Parental Supervision Restricted Messaging Private Mode	Followers visibility Zooming Profile Picture Single Sign-On (SSO)
Snapchat	Customised location visibility Screenshot notify	Location Feature Ephemeral communication
WhatsApp	End-to-End Encryption Contactless messaging QR code security	Unrestricted Messaging Open group invitation
Google	Google Safety Features Password Manager(easier to remember) Find my phone	False positives spam filtering Password Manager (May leak credential information)
Youtube	Minimal personal data Contactless	Not mentioned
Imo	Not mentioned	Unauthorized contact visibility Unrestricted Messaging
Apple	Find My Phone	Not mentioned
Mozilla Fire fox	Ad Blocking	Not mentioned

Table 7.1: Participants' trustworthy and untrustworthy security features in various apps and websites.

creating complete passwords and avoiding saving passwords in shared devices should also be adapted as a habit. After encountering with credential thrift participants realized and suggested not to share their credential information with others.

> *"Many of criminals ask or take OTP in a manipulative way, never share that."* - US2

Similarly, as all of our interview participants faced one or many cyber threats, their reported suggestion is mostly about avoiding and being cautious of those faced threats. Such as, avoiding suspicious and tempting links that come with offering prizes, discounts or easy ways to earn money as these are mostly mapped to steal personal data.

> *"Beware of tempting offers that ask for clicking in a link, only reliable sources should be accessed with verification."* - US4

Furthermore, a repeated concern was about deep fake videos and Ai modified images. As this is misused widely for blackmail and harassment. Seeking expert help when needed is emphasized by participants because according to them, most of the women do not know how to overcome the risky incident and afterwards they also hesitate to share their issues with others to solve them.

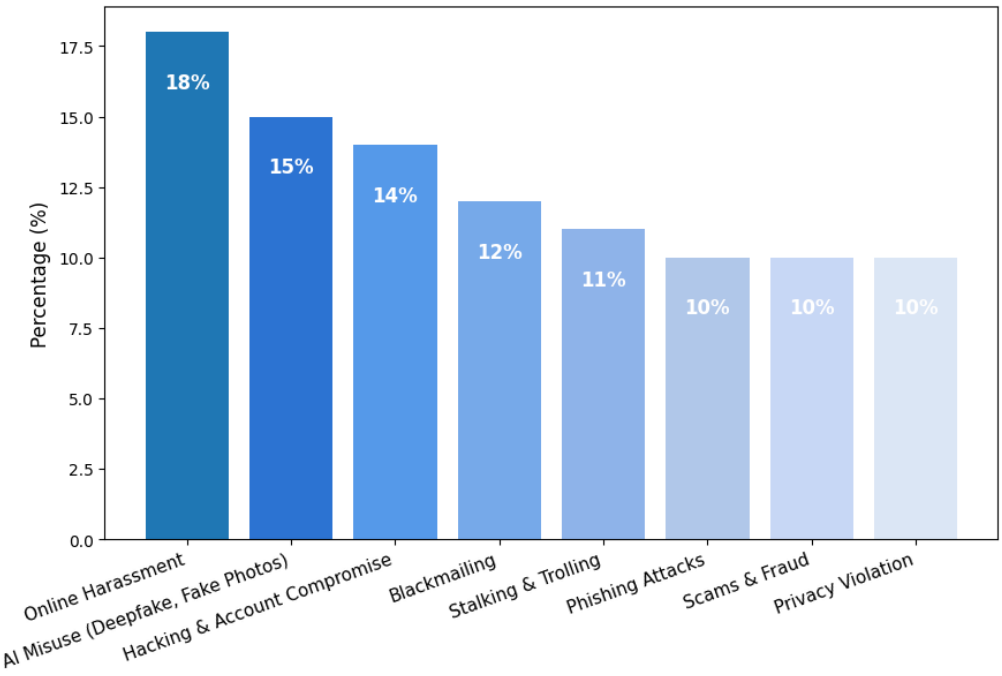

Figure 7.6: Women's perspective on online threats targeted to women

7.3.4 Women's Suggestions on Enhancing Cybersecurity Awareness and Education

The responses from participants highlight a collective suggestion of educational resources or training that would be most effective to them to improve their cyber security awareness knowledge. Most of the participants emphasized on the importance of introducing cybersecurity awareness in educational institutions and the workplace. They particularly focused on educating women about phishing, hacking, online scam and privacy management. HS1 stressed about her preference for a cyber security education.

> *"In every school a class should be held about cybersecurity. So that I can have a clear understanding about the idea of hack, spam and can protect myself."* - HS1

Furthermore, educating parents about cybersecurity is important so that they can guide their children on safe internet usage. To highlight on this W1 shared,

> *"As from the primary stage students are going through a learning process, for that from school level they should get educated about cyber security and aware of potential risk. Guardians should also be trained up, so that they can give guidelines to their child."* - W1

As well as the social media awareness campaign is a great source advised by participants to share cybersecurity awareness knowledge. Involving celebrities to promote cybersecurity awareness knowledge can encourage the younger generation a lot. Reels, posts and advertisements attract participants prominently, so they choose to get educated through these platforms. Designing a cybersecurity awareness program and workshop both for urban and rural women is prioritized greatly.

"It will be very helpful if we design something for rural women to build their awareness." - US12

In addition to this, participants also suggested that designing animated videos and online courses can help them to learn more about cybersecurity concepts. Strict policy and law enforcement against cybercrime is a need to all.

On this note, these findings indicate the necessity to build a safer online environment for women with a comprehensive cybersecurity awareness knowledge. These findings indicate a call for a complete framework to women to support them intensively into their cybersecurity knowledge and practice. Ranging from educational resources, videos, communication platforms, workshops to global support systems that thoroughly help women to build a great impact in their cybersecurity awareness knowledge.

7.4 Technology Readiness

The technology-readiness refers to people's tendency and preparedness to embrace and use new technologies for accomplishing goals in home life and at work [8]. It is a concept of overall state of mind resulting from positive and negative thoughts about technology. Together this indicates a person's openness to use new technology and innovation. At the end of our interview session, we provided the participants with a TR questionnaire. That contains two sets of questions, one for the positive attitude and another for the negative attitude toward technology acceptance. The questions were in likert scale ranging from 1 to 5. Each of the 30 interview participants attended the TR questions. The questions are provided as following:

- **Optimism**
    1. Technology helps me do tasks on my own without needing help from others.
    2. Technology allows me to complete my tasks faster and efficiently.
- **Innovativeness**
    1. I desire to explore new applications, websites, and technology as soon as they are available.
    2. I am great at advising others about using any new technology.
- **Discomfort**
    1. I feel uncomfortable using digital platforms that require sharing personal information.
- **Insecurity**
    1. I often avoid using online platforms that have online payment methods.

To measure the internal consistency of how closely related the items are in each group, Cronbach's Alpha is used. It checks how well a set of questions (items) measure the same concept. We divided our respondents into three groups. Since our sample size for the Cronbach's Alpha test is small, $\alpha \geq 0.6$ is considered an acceptable range [50]. Furthermore, to evaluate whether TR differs among 3 Groups: ANOVA test is conducted. It compares TR scores across 3 groups of participants. By ANOVA test we determine if there are significant differences in TR scores across groups. In ANOVA test if p value is $p \leq 0.05$, there is significant difference in TR across the group. If $p \geq 0.05$ the group have similar TR levels, meaning no significance difference.

The F-value in ANOVA measures how much the groups differ from each other. A higher F-value means there is a bigger difference between the groups. If F is large and $p \leq 0.05$, the difference is statistically significant. If F is close to 1 and $p \geq 0.05$, the groups have similar TR levels, meaning no significant difference. Table 7.2 shows the result of TR evaluation.

Metric	**Positive TR**	**Negative TR**
Cronbach's Alpha (α)	0.6510 (Acceptable)	0.6076 (Acceptable)
ANOVA F-Value (F)	1.3518	1.0175
ANOVA p-Value (p)	0.2757 (NS)	0.3749 (NS)
Interpretation	Similar TR	Similar TR

Table 7.2: Cronbach's alpha and ANOVA results for TR analysis (NS = Not Significant)

The result of TR indicates that the internal consistency of our TR items is in acceptable range for both positive and negative TR and there is no significant difference among three groups. All groups have similar TR levels. No group stands out as having significantly higher or lower scores. This indicates that the difference of educational level or job status between the three groups does not strongly affect how someone is ready to adapt to new technology. So, here it seems that all three groups have similar TR levels. This suggests that all three groups of women participants, high school students, university students, and working women exhibit a similar level of willingness and preparedness for adopting new technology. Therefore, our TR result suggested to the future work that new technological advancements can be adapted equally by all groups.

Chapter 8

Discussion

Our survey results from Chapter 5 and interview results from Chapter 7 effectively address all of our research questions. Our analysis provides an understanding of the current state of cyber security awareness among Bangladeshi women through an intensive survey. Secondly, exploring through interviews we uncovered the potential risks and threats faced by women due to their cyber security awareness level as well as the human behaviour and situational factors that influence users to engage in risky cyber decisions. Finally, analysing the findings of these areas our research proposes a design intervention to bridge the gap of low cyber security awareness among Bangladeshi women.

8.1 The State of Cybersecurity Awareness Among Bangladeshi Women

This section effectively addresses the current state of cyber security awareness among Bangladeshi women obtained from Chapter 5. By thoroughly examining findings of five factors from the survey, we are able to assess how women navigate in the digital landscape. Identifying their password security, information security, device privacy, their response in incident reporting and their ability in malware detection we found how women of three demographics provide insight on their protective measure and their level of awareness in cyber security. Table 8.1 shows a summary of knowledge level across the five factors among the three women group.

8.1.1 Demographics

On analyzing the three targeted groups – high school students, university students and working women, the results of the demographic sector provide us a deep insight of their background of living and their current life status. This survey portrays a strong data set of each group but there is significant disparities in response of each group based on the factors. As our three targeted groups of participants are from different age groups and backgrounds, there is a significant gap of knowledge as well. Nowadays, most of the school students have their personal device, that's why the tendency of them getting cyber attacks is high and cyber knowledge is very important to them [91]. Moreover, the rural and semi rural women also spend a significant time on digital devices but the resources of them knowing about cyber

security is less [59], which leads them to a vulnerable condition. Figure 8.1 shows the distribution of time spent in digital device by group. It is also noticeable from our results that university students have the tendency to use the highest time such as more than 6 hours on a digital device.

Question	Group	Mean Score	Awareness Level
2FA Usage	High School	2.20	Low
	University	3.11	Better
	Working	2.55	Moderate
Password creation	High School	2.74	Moderate
	University	2.83	Moderate
	Working	2.59	Moderate
Phishing Knowledge	High School	2.09	Low
	University	3.52	Better
	Working	2.28	Low
Device sharing	High School	2.74	Moderate
	University	2.99	Better
	Working	2.78	Moderate
Public Wifi	High School	2.60	Moderate
	University	2.73	Moderate
	Working	2.24	Low
Steps on security breaches	High School	2.79	Moderate
	University	3.10	Better
	Working	2.53	Moderate
Download Cautiousness	High School	2.74	Moderate
	University	2.89	Moderate
	Working	2.58	Moderate

Table 8.1: Cybersecurity awareness knowledge across group

8.1.2 Password Security

The results from the descriptive analysis of section 5.2 reveals that the high school students have a good practice of avoiding password reuse. On the other hand, the majority of students have a tendency to use personal information as a password. It has been well established that passwords that include elements of personality to them can be easily cracked using specific methods such as a dictionary attack breaching user account [87]. We also found high school student have the tendency to writing down password in a unprotective way. In a prior research [7], they have also worked on password security, uncovering that, about (35%) people have the tendency to write down their passwords in insecure places, such as in wallets which make them vulnerable. Although, it is shown from the result that school students have a higher knowledge gap in 2FA practice than university students. Among all groups, university students seem to have more practice of using 2FA in password. Furthermore, for working women there is an average level of awareness in using personal information in passwords. On the basis of the confidence level of feeling the password strong, university students claimed to be more confident than the other two groups. After observing the above data we decided to test our hypothesis

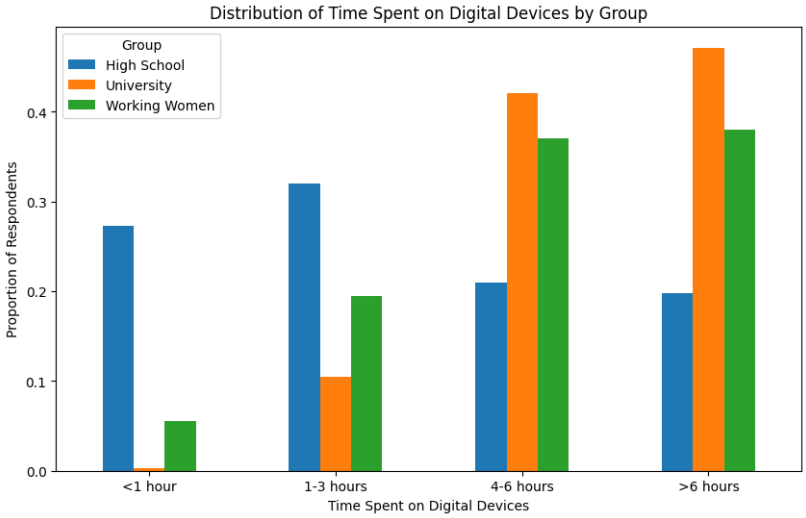

Figure 8.1: Time spent on digital device daily : three groups

1, which is that women who reuse passwords across accounts might be less likely to consistently use 2FA. We had the assumption of high percentage of re-usage of password and low percentage of 2FA but our hypothesis results indication that the in reality of three demographic groups proved us quite wrong because one group (High school) had the largest number of people never reusing the same password nor using 2FA, another (University) had highest number of people using always using 2FA while mostly reusing password and other (working) always uses 2FA while never using the same password. Based on our findings in password security, it demand for a effective and secure password usage education for women to safeguard their personal and sensitive information.

8.1.3 Information Security

The results of information security from section 5.3 shows that the school students have very little idea about phishing. A significant number of students claimed that they had never heard of phishing, while a small segment of students claimed to be aware and knowledgeable about it. On prior research it can also be seen that, women are more susceptible to phishing attacks compared to men [29]. As our finding shows that high school students have less phishing knowledge, then it can be said that their chances of getting attacked is higher. On the other hand, from the Table 5.14 of university student's, it is shown that they are moderately knowledgeable about the phishing concept. While identifying the actual result of the phishing example high school students seem to have a low knowledge. As well as, the Table 5.15 from the working women, it is shown that they also have a vulnerable phishing knowledge. From our survey response, we found that a very small number of women have already attended cyber security awareness training/seminar/ workshop. And the majority of women expressed their interest in attending in the future. The findings highlight the critical gap in phishing awareness and the inaccessibility of cyber security awareness training, seminars, and workshops. An urgent and structured response to these can develop a transition to the gap.

8.1.4 Device Privacy

From analyzing our statistical analysis of device privacy knowledge and practice for the all group, section 5.4 shows the result for all groups. From the Figure 5.4 it can be state that, university students have less tendency to share their devices and working women and high school students are more frequent in sharing devices. It portrays that there is a privacy leak tendency of one's personal device due to multiple sharing. It has revealed that in Bangladesh, women are being forced to share their mobile phone with husbands or other family members without mutual access [68]. Thus, device sharing with family members has led the women members of the family in a privacy violation. Moreover, from our analysis, when it comes to reviewing or adjusting the app permission, high school and university students have more practice than working women groups. On the basis of awareness on using public Wi-Fi, university students are more aware. Whereas, the other two groups are less aware. This lack of awareness can be threatening for their devices. It is important to mention that, on device privacy protection all three groups showed that they are mostly habituated with using strong protection methods. The high school students mostly use a password/ pin. But It would have been a more secure method of protecting devices using both biometrics authentication and password. In a prior research [68], it shows, there is a dearth of work in information privacy in Bangladesh. For example Dhaka's repair market, the shopkeepers mishandle the customers' information for their benefits. Which clearly indicates the risk of not having a proper device privacy protection.

8.1.5 Incident Reporting

Analysing the Incident reporting factor, the result shows that high school students have experienced cyberbullying most. It makes them highly vulnerable. From prior research, it is highlighted that, reporting cyberbullying incidents to the authorities helps to reduce the number of cyberbullying incidents [43]. In our analysis among the all groups, university students appear as the group with the highest number of reported cyberbullying cases but others do not. In response to their action to take any cyber security breaches and confidence level of handling cyber attack, university students have emerged with more knowledge. After observing these results, we decided to test our hypothesis 2 in section 5.5.4 which analyses the confidence in women's ability to handle cyber -attacks correlates with reporting cyberbullying incidents. The second hypothesis proved our assumption on confidence about integral regarding reporting on cyberbully incident, as we observed that when the level of confidence is 5, high school, university and working women has 22.78%, 65.65% and 53.86% probability of reporting respectively whereas when confidence level is 0, the respective group has 12.62%, 30.02% and 17.88% of reporting. Hence from the results, we can see they are proportionally related as when level of confidence increases, so do the chances of reporting cyberbully incidents.

8.1.6 Malware Detection

From the analysis of malware detection factors, it can be indicated that the working women participants are the most vulnerable in the malware detection knowledge. The working women are comparatively less cautious about downloading academic

papers/games/movies from unknown sources. The experience of using malware detection tools is shown in Figure 5.5 and the frequency of them using it is less in high school students and working women than university students. Thus, it can be said that university students have a better knowledge of malware detection and prevention. To have more insights into malware detection knowledge of the three groups we test hypothesis 3. That women's field of study and employment correlates with their ability to identify phishing examples and malware detection on their device. But this third one proved us completely wrong. Initially we assumed the field of study/area of employment was relevant with awareness of malware and phishing threats but our analysis showed that the study/ area of employment does not have any significant effect on awareness of such threats.

The findings from our study underscore the urgent need for structured learning resources and explicit attention to password security, information security, device privacy, incident reporting and malware detection. A factor specific approach with in depth practical suggestion and direction can navigate women in the digital landscape securely. A women inclusive cyber security framework need to established to provide them with digital literacy. Educational resources on these factors will empower women with confidence and competence required to enhance their cybersecurity awareness knowledge.

8.2 Assessing the Cybersecurity Awareness: Risks and Threat Faced by Women

From Chapter 7, a deep-driven analysis provide understanding on risk and threats faced by women in Bangladesh. The increasing attacks are mostly surrounded with women that resonate with prior research that the females are more vulnerable to cyber-attacks [52]. Our finding reveals that the digital environment is noticeably vulnerable for women and focusing on their digital literacy is undervalued in our country.

8.2.1 Women's Understanding on Cybersecurity

Cybersecurity awareness is understanding about the knowledge of cyber or information security aspects. [79]. From the findings of our interview we relieve a divergent level of cybersecurity awareness among our participants. Extending from limited knowledge to a better understanding of security and privacy practices. Their response highlighted that many participants do not entirely feel they are properly adequate with the cybersecurity awareness knowledge while some understanding indicates proactive approaches to securing themselves. Their perception on cyber security awareness is more in behavioral action rather than understanding it is a digital hygiene practice. After analysing their understanding on cyber security awareness emphasise on the essential need for cyber security awareness and education in Bangladeshi women.

8.2.2 Women's Experiences with Emerging Cyber Threats

With the progressive increase in the number of internet users in Bangladesh, the percentage of attacks is rising too [108]. From our findings Figure 7.1 it is revealed a multifaceted landscape of cyber security risks and threats encountered by women. Phishing attacks, account and identity compromised, malware attack, scam, vishing, online harassment and more obstruct women in the digital environment and create an unsafe environment. When women of our country are leading more to the digital usage and cyber world, cybercrime is a derivative of ever-increasing development in the areas of information and communication technology [54]. From our findings it is revealed that social engineering tactics greatly perform in driving women to risks and threats. One of the most prevalent risks identified are phishing attack, hacking, scam and identity theft which affect most of the participants. But the findings demand discussion that these women do not really possess any knowledge on phishing, identity theft, data breach, malware, ransomware and other threats until and unless they face these risks even once in their life. This is crucial to address that all these growing threats are notably observed in their experience of digital usage while they were unable to overcome the threats. Even today when we analyse their security and privacy related unwanted incidents we find, they still go through vulnerabilities and fragile security environments and are clueless on handling these risks and uninformed of where to seek help. These findings underscore a clear cybersecurity awareness gap among Bangladeshi women. The inadequacy of security and privacy knowledge is mostly responsible for emerging risks and threats. These insights urgently call for improved digital security and privacy practice guidelines on these most frequently engaged risks. Therefore, women of Bangladesh can be digitally protected and be literate on imminent risk.

8.3 Behavioural and Situational Factors Influences on Risky Cyber Decision

The findings from Chapter 7 reinforce that women being victim of cyber attack is not solely a result of lack of awareness but also influenced by behavioral tendency and situational vulnerability. Cybersecurity must not be addressed by only technology. Rather, it is deeply intertwined with human behavior and decision making [64]. Therefore, we found valuable insight on human behavior and situational factors influencing women to engage in risky cyber decisions.

8.3.1 Human Behaviour and Situational Factors

Our findings from Figure 7.2 reveals that human behavioral patterns and situational factors significantly correlate with cybersecurity risk. While personality is widely studied in psychology literature, few studies examine the relationship between personality traits and security behaviors [51]. Bridging this gap our findings evaluate by categorizing the women's narrative. We found key findings that influence them to be associated with security and privacy risk. Unconscious and negligence on digital security is the leading human behaviour that is increasing exposure to cyber threats. Findings highlighted that participants overlook security measures that include two factor authentication, password updating and scrutinizing unknown messages. Our

findings suggest cognitive bias, where women overconfidence often led them to underestimate the risk. This aligns with a prior study that individuals who consider themselves as less vulnerable to cyber threats, tend to take less cyber security precautions, thereby increasing their exposure to risks [25]. Temptation and instant gratification also adversely affect security measures. The drive for immediate rewards influences them to override rational decision making. Because of having limited security and privacy practice panic and fear responses emerge as a critical factor where we found participants sharing their credential to unknown sources. Women who prioritized immediate results over careful verification are found as more vulnerable to risks. Moreover, convenience over security is also a predominant human behaviour leading to increased susceptibility to various attacks. Curiosity driven risk is also a significant behavioral choice that women take upon themselves, later resulting in compromised their security. Finally, overtrust and blind faith is also repeatedly observed in our findings, through that women make them set apart from the reality and get associated with potential risks. Overall these observations highlight a relation between human behaviour and cybersecurity threats. Enhancing cybersecurity resilience requires an awareness that will engage human attention so that they can grasp their behavioral tendency that are responsible for cyber attack.

8.3.2 Vulnerabilities Tending Women to Cyber Attack

Nowadays, the cybercriminals mostly target humans rather than machines by exploiting the weaknesses of end users to achieve their goals. That is the reason why human vulnerabilities have become a significant threat as their security and privacy is being hampered [80]. Women also face these vulnerabilities while associating with the cyber world. From our findings in Figure 7.3 we perceive that there is significant lacking and inefficiency among women which influence their exposure to cyber risks. Insufficient awareness has been reportedly mentioned by our participants as they highlighted many times that they do not have basic knowledge about cybersecurity risks. Many participants shared their personal details, such as one-time passwords (OTP), without realizing the risks associated with such actions. Digital illiteracy further compounds these risks, as women struggle with the essential skills required to identify and manage cybersecurity threats. There is a significant gap of their understanding in digital literacy, particularly when it comes to identifying trusted sources and maintaining a safe digital environment. The further important aspect is the widespread occurrence of weak security practices among women. Women tend to fail in the implementation of basic security measures like enabling two-factor authentication (2FA) or using strong passwords. Also some of the interviewees also exhibited their poor privacy control which also is an exposure to cyber risks for them. Oversharing personal information on social media is one of the compromises made by women as they sometimes do not understand that by doing this behaviour online might lead to identity theft, phishing attacks, or unauthorized access to sensitive data. Lastly, the absence of familiarity with security features is a fundamental weakness which adds to the women's exposure to cyber dangers. Women are unaware of available security tools or did not know how to use them properly, causing them to have preventable cyber incidents. By analyzing their vulnerability, it is clear that the gaps of their understanding while associating with any cybercrime makes them more vulnerable in the cyber world. Minimizing these gaps in vulnerability

would make women more aware and will also help them to secure their privacy and security.

8.3.3 Women's Understanding on Security Warnings

From our observed data in Figure 7.4 it is evident that the participants frequently disregard security warnings. Which reveals a concerning tendency taken by women, proceed toward unprotected cyber space. Despite being aware of security warnings the majority of women exhibit their behavioral tendencies over security preference. Through categorizing the rationale our finding explicitly reveals that desensitization, dismissal of pop-ups, excessive dependency and trust in source are the main grounds to ignore security warnings. Desensitisation is observed as the most prevalent factor where participants ignore warning as finding it as a routinely alert because of habitual exposure. The frequent security warnings lead to exposed reduced sensitivity to actual threats. This prone to dismissal is particularly evident in women engaging in unsafe downloading, skipping to read terms and condition agreement, where security warning is considered as a regular message rather than proactive measure. Moreover, dismissal of pop up warnings, where women prioritize their convenience of security. The pop warning tends to be an interruption in their usage, as they ignore it rather than taking it in their action. Such as a user dismissing a weak password alert, thus makes her vulnerable to security threats. Excessive dependency on digital platforms developed as another key behavioral factor influencing women in security warning negligence. Our finding highlights women justified their compromisation on security warning due to excessive dependency over their used platforms. This finding emphasises that women repeatedly choose on dependency due to perceived lack of alternatives. As well as this outcome aligning with the behavioral response where fear of missing out information carry out a role for engaging them is a risk taking decision. Women's bias behaviour into trust in source also found out to be a critical factor to ignore security warnings. Trusting on google play store, recommendation and known contacts violated their data as they choose to ignore warnings considering all to be trusted sources. From the finding it reveals a core gap between security awareness and behavioral compliance. To address this issue it requires approaches that integrate with behavioral design principles. An approach mentioned in [39], where they found that polymorphic warnings, which change in appearance, can effectively reduce habituation in the brain, thereby enhancing the effectiveness of security alerts.

8.3.4 Decision Making in Cybersecurity Threats

Based on insight from Figure 7.5 indicate that women's action and inaction towards their encountered risky incidents. Our finding shows a higher rate of choice in not taking action against their cyber threats which highlights women's decision paralysis in cyber security. Among the participants it adversely shows that, It is observed by our analysis that reasons behind not taking any action to their threats. Users could not primarily identify what kind of threats or attacks they faced; they do not understand what action is needed to take for that incident. As well as other factors such as fear of parents on youngsters is also backlogging them to take any action. On the other hand, there is low adoptive measures like two factor authentication

despite encountering threats. Moreover, while reporting to responsible authorities some of them found no assistance and guidance which actually shows the limitations of existing helplines and support systems. The tendency of escaping the incident by blocking and deleting without adapting any security measures in their usage shows the inadequate knowledge of women. The current barriers to handle online abuse were related to lack of awareness of users as well as in the cyber tribunals mentioned by an existing work [82]. Similarly, from the findings it is evident that there is no trustable platform, where women can seek help and acquire knowledge regarding cyber security awareness and practice.

8.4 Strengthening Cybersecurity Awareness: Practical Approaches and Recommendations

This section covers details to enhance cybersecurity awareness across Bangladesh. As seen in Chapter 5 and Chapter 7 the women of Bangladesh from high school, university and working professionals exhibit inadequate cybersecurity awareness and a limitation of understanding security and privacy practice. Women's insufficient knowledge on digital safety measures, online risk and threat detection and limited understanding of secure internet usage expose them to vulnerable cyber attacks, including phishing attacks, online hacking, identity theft and data breaches. Therefore, strengthening cybersecurity education and supporting safe digital habits is vital to empowering women of Bangladesh.

From our findings it is evident that high school students are increasingly exposed to cyber space without proper knowledge on digital security and privacy. Often they associate risk without understanding privacy settings, safe browsing and leaving their personal data inadvertently in digital spaces. To address these concerns an integrated cyber security curriculum is necessary or emphasizing on cybersecurity knowledge through ICT courses is necessary. Providing digital literacy will highly contribute to shaping a secure cyber environment. As well as, for university students and working women interactive workshops, seminars and awareness sessions on digital and online safety can impact profoundly on their cybersecurity knowledge. Age specific awareness programs should be implemented rather than one size fits all approach. For high school students conducting a workshop explicitly on strong password management, demonstrating the importance of two factor authentication, knowledge of phishing, malware, device privacy protection and privacy setting on social media will be highly practical to learn about these factors effectively. As well as mandatory training and awareness programs must be developed for working women or for critical sector employees. To implement this, the government can build partnerships with cyber security firms and provide training to working women at regular and appropriate intervals. Moreover, public awareness campaigns through social media, TV and celebrity personality would reach a wider audience. Establishing cyber security boot camps and mentorship programs for youth and career professionals can highly motivate them to build a safer digital space. To overcome emerging cyber threats, collaboration between the public and private sector is important so that more powerful projects are organized to address cyber security awareness. Finally a strong cyber law and better enforcement to protect women dig-

itally in Bangladesh is in critical need now. Women across urban, semi-urban and ruler ask for an authority to take quick action against their cyber attacks. By fostering a cybersecurity-conscious nation, It can ensure that women of Bangladesh are empowered with knowledge and tools to safeguard their digital security and identity.

Based on our study findings, which involve conducting surveys and interviews, we identified critical gaps in cybersecurity awareness on women that need urgent attention and resolution. Women not only demonstrate their lack of essential knowledge but also express their need for a more self-directed approach to learning, enabling them to enhance their cybersecurity knowledge. Recognizing these findings we propose a framework that will develop cybersecurity pathways and a comprehensive understanding to create and spread awareness across women of all demographics in Bangladesh. This framework aims to overcome the knowledge disparities and empower women with skill and navigation. The details of the proposed model is discussed elaborately in Chapter 9.

There are many existing works in the field of cybersecurity awareness but very few are women based and specially no work on covering a wide age range of women's cyber security awareness has been conducted in Bangladesh. Exploring through three different demographics covering the wide area of our country, we provide a detailed examination on women's cybersecurity practice and knowledge. By implementing a large-scale survey and interview we assessed the cyber security awareness among different groups of Bangladeshi women. We systematically examine occuring cybersecurity threats encountered by women. Our work identified women as a victim of cyber attack is not merely a consequence of limited awareness but also influenced by behavioural patterns and situational vulnerabilities. We identified women's understanding of security warnings and their decision making pattern to the cyber threats. Our findings also reveal potential barriers for women to address their cyber security related threat. We address women's insights on security, privacy and digital policies across their digital experience. Based on research findings we propose a framework to overcome the knowledge disparities. This work contributes to the HCI community by integrating women's cybersecurity awareness knowledge, their faced cyber threats, behavioral influence and situational factors to inform the design and reformation of cyber security awareness education and intervention.

Chapter 9

Proposed Framework

This chapter overviews the current cyber security awareness and learning sites in Bangladesh and their effectiveness. Furthermore, it will explore the proposed framework detailing its features and how it may have a potential impact in fostering knowledge to prevent cyber malpractice and improve cyber hygiene.

9.1 Existing Frameworks

Cybersecurity models which are usually used in cases of cybersecurity and awareness, often based on are:

- **Cybersecurity Awareness Framework**
  - Prioritize user education through campaigns, training sessions, or institutional initiatives. Notable examples are the Protection Motivation Theory (PMT) which is focused on four major elements that are vulnerability, self-efficacy, response efficiency and severity [2]. Another example is the Theory of Planned Behaviour (TPB) which has major three core that are attitude, subjective norms and perceived behavioural control [4]. Ultimately, both of the frameworks comprises of elements which highlight the psychological and behavioural aspects that affect cybersecurity practices.
- **Risk Management Framework**
  - It prioritizes risk identification, risk measurement, risk reporting and monitoring and risk governance; One of the example of Risk Management framework is NIST which is often used to assess, mitigate and eliminate threats. It can be observed that NIST framework comprise for 5 elements which are Identify, Protect, Detect Respond and Recover. This highlights the effectiveness of implemented knowledge to detect, response and mitigate threats in a manner to reach an outcome through systematic process[58].
- **User Centric Design Framework**
  - It prioritizes user's action and navigation; ensuring the flow remains smooth, easy and comprehensible, minimizing cognitive lead with high

adaptivity to diverse needs via iterative feedbacks intuitively highlight the psychological and behavioural aspects of user actions.

9.1.1 Existing Sites in Bangladesh

These are some of the sites in Bangladesh that promote cybersecurity contents. Most of them can be grouped as following Cyber Awareness framework with their focus area being *Career Training* or *Awareness*. One of them can be grouped under Risk management framework with its focus being on *Incident Reporting* .

Website Name	**URL**	**Focus Area**
Cyber Bangla [67]	https://cyberbangla.org	Career Training
Bangladesh Cyber Institute[33]	https://cyberinstitute.com	Career Training
Creative It [17]	https://creativeit.com	Career Training
Inspira [89]	https://Inspira.com	Awareness
BDG e-Govt CIRT[40]	https://cirt.gov.bd.org	Incident Reporting

While the websites 9.1.1 do offer branch of knowledge but it's contents are steamlined learning for Career based implementation for adults and students in IT industry, not for general daily practise and consumption. Which means these are not accounting the socio cultural norms of Bangladesh. Hence we chose our model to be user-centric to aim to reflect the socio-economical culture for diverse group of women present in Bangladesh.

9.2 Proposed Framework

Our proposed model aims to address the cybersecurity awareness gap among Bangladeshi women by integrating specific features designed to meet their unique needs; knowledge of cybersecurity practice for awareness and enable them to develop themselves to maintain cyber hygiene to attempt prevention of falling under risks and, if they do so, how to calmly mitigate the problem to reach an optimal solution. Our chosen model for intervention is a high-fidelity prototype mimicking an e-learning advocacy website for cybersecurity. The reason an prototyping was chosen over website is because of the following reasons given below:

- Flexibility in design: It is easier to adjust and modify User Interface to enable smooth User experience and it is simple to change user flows to meet up with design iteration according to user feedbacks
- Ease of manage functionalities: It allows to display how features would work in visual ways without the complex implementation of full backend system which would be need in website. It also helps to minimize redundancy of elements by allowing the testing of critical cybersecurity awareness knowledge and the refinement of features.
- Avoid scope creep due to limitation of data in rural areas- By prototyping, most of the functionalities are kept lightweight and focused on core features keeping the design efficient and applicable in urban and rural areas.

Overall, prototyping was chosen for its flexibility to change and easier implementation of visual workflow of user flow.

9.2.1 About Prototype

The prototype 's goal is to make these materials easily searchable by guides, tutorials, and other aids and real-time help to shield women and students online. These features include the ability to engage the learning sources and tools on various areas of interest like passwords, phishing emails, and many more, the ability to communicate to get answers to any immediate questions or feelings, get various challenges and practices, formation of community forums, and among others, other available resources. including guides, tutorials, and real-time support, to help women and students protect themselves online. The website features may include interacting with learning sources and tools on different topics such as password management, identifying phishing emails and etc, communicating to get answers to any immediate questions or concerns, various challenges and practices, establishing community forums, and other accessible resources.
Prototype link https://she-build.org from Figma

9.3 Features Description

The features of the prototype are listed and described in below:

- **Video Tutorials:** Video tutorials serve as the fundamental element of the website since they provide cybersecurity education in both English and Bengali language The video tutorials of the website present information on Password Security, Information Security, Device Privacy, Incident Reporting and Malware Detection. Different skill levels among users can access the website through Beginner, Intermediate and Advanced structures. The content of the website aims to serve students at all grade levels and working women by offering learning materials at suitable difficulty levels. The tutorials include practical examples with step-by-step guidelines to make learning both educational and directly applicable. The feature serves as a digital literacy solution for Bangladeshi women to confidently apply essential cybersecurity practices in their real-life activities. Figure 9.1 visualize the video tutorials feature.

Figure 9.1: Video Tutorials

- **Event, Workshops and Seminars:** The platform functions as an online bulletin board to promote upcoming cybersecurity education activities which take place throughout the world and across local communities. The platform presents both virtual and physical gatherings which enable female participants to join skill development sessions that showcase current cybersecurity practices. This information access proves essential for women who live either in rural or semi-urban regions of Bangladesh which face limitations in their cybersecurity resource availability. Attending these events delivers expertise growth and generates professional connections which connect women with cybersecurity specialists as well as their professional peers. Figure A.2 visualize the video tutorials feature.

- **Cyber Incident Updates:** The section contains recent reports and case examples regarding genuine cyber incidents along with details about data breaches followed by descriptions of phishing attacks and malware outbreaks which is provided by our users whoever has experienced and witnessed it. Through this feature users acquire knowledge about potential dangers plus learn effective prevention methods against these incidents. As others can view this and know about the concerning details, digital crimes and prevention shared by the users can help them learn and prepare them toward defending themselves online. Figure A.3 visualize the cyber incident feature.

- **Discussion Forum:** Users can participate in the discussion forum which serves as an interactive environment where they can safely exchange dialogues about cyber events or best practices with their peers. It is more like a chatbox where women users can connect with members while expanding their community and discuss their security experiences in addition to obtaining information about their cybersecurity issues. Figure 9.2 illustrate the discussion forum feature.

Figure 9.2: Discussion forum

- **Testing Tools:** The testing tool feature in Figure 9.3 shares direct links to multiple safe cybersecurity testing instruments including phishing link verification tools and malware detectors which users can access at no cost. The tools provided allow users to test their online security while also obtaining methods to prevent potential dangers. Such a feature enables Bangladesh-based women who lack technical expertise and limited resources to obtain digital safety-enhancing tools conveniently. Through this feature users obtain

the power to protect their cybersecurity and keep their devices alongside their accounts safe.

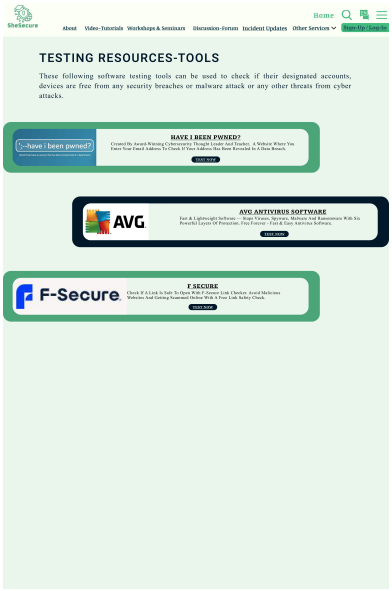

Figure 9.3: Testing tools

- **Expert Consultation:** Users of expert consultation platform shown in Figure 9.4 can reach out to security consultants with experience through the expert consultation feature to solve particular issues or address questions. This feature serves to be effective for those who want to take one-to-one consultation for any particular problem and also for those who feel more assured while talking to our experts. The expert consultation feature serves as an essential resource for Bangladeshi women because they normally do not have access to professional cybersecurity services and can use this service to build confidence and discover suitable methods to prevent cyber security risks through individual consultations.

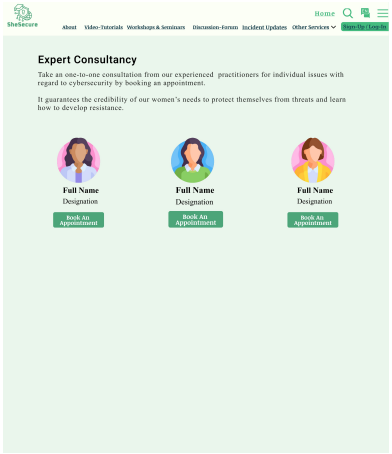

Figure 9.4: Expert consultation

- **Quizzes:** Users can assess their cybersecurity knowledge through the quizzes which create evaluation opportunities for different subjects. The quizzes use

beginner, intermediate and advanced tags to group questions which create an engaging method for users to test their knowledge. Users can find their knowledge gaps because of immediate feedback and explanations which furthermore encourages more learning. Through this platform element Bangladeshi women can develop progressively while gaining assurance about their digital world safety skills. Figure A.7 visualize the quiz feature.

- **News and Articles:** Users can access the latest updates from the cybersecurity world through this section which covers new security threats as well as technological advancements and profiles of women in cybersecurity work. The platform maintains user engagement through its various content selection which serves to inform and motivate users. Through this feature Bangladeshi women receive information that fills their cybersecurity knowledge gaps which motivates them to begin careers in cybersecurity fields while learning how to protect their digital security. Figure A.8 visualize the news tutorials feature.

- **Help Desk:** This feature enables our users to resolve technical issues, difficulties and request website maintenance or ask questions about website capabilities. Users have quick access to help through contact details that include email and contact details. Figure A.8 visualize the news feature.

9.4 Intervention and Recommendations

From interview and survey results, we can observed there is a lack of promotion of cybersecurity awareness practise which has led many people to not know about good cyber security hygiene. It can be solved by the following:

- **Cybersecurity Campus Ambassadors Program**
  - Train female students from various departments regarding cybersecurity hygiene, risk mitigation and tools; encouraging them to teach their fellow peers to foster confidence and growth of cyber resilience .
- **SMS based cyber campaigns**
  - Send SMS in Bengali to send cyber security tips for those with inadequate internet connection. It would help to promote cybersecurity awareness in rural areas where is not adequate internet connection.
- **Offline Resources**
  - Distribute offline materials and posters in localised contents which would be familiar to related to in rural areas to foster the importance of cyber security practises.
- **Social Media Awareness Post**
  - Promote cybersecurity awareness posts and videos in social media. Hold online poster competition regarding Cybersecurity awareness Infographics to induce social engagement amongst people.

Chapter 10

Conclusion

10.1 Summary

By conducting a comprehensive study on three demographics of Bangladeshi women: high school student, university student and working women our work presents an in-depth analysis on women's cybersecurity awareness knowledge. For our research we collected data in two phases: survey across different regions of Bangladesh employing google form and in-person paper survey; another is semi-structured interviews. Our work initially assesses the cyber security awareness knowledge and practice based on five factors: password security, information security, device privacy, incident reporting and malware detection. To analyse more extensively and justify our survey result we conducted semi-structured interviews covering more of women's practical understanding of cyber security knowledge and digital usage. In the interview, at first our work found most encountered cyber threats by women. To understand the background reason of these prevalent risks faced by women, we perform further examination where we found human behaviour and situational factors also correlated with low cybersecurity awareness of women to influence them in associating with risks and threats. Additionally, our findings highlight women's perspective on security and privacy features along with policies governing their digital usage and experience. Furthermore, our work identified key barriers that hinder women to effectively address their cybersecurity threat. To overcome all these disparities, we finally propose a framework aiming at enhancing cybersecurity awareness knowledge among Bangladeshi women.

10.2 Limitation

Our work is limited by a prototype rather than a fully functional systematic website. Additionally, our work do not includes more women from working professionals than the other two groups due to lack of support from various workplace's internal hierarchies. Furthermore, in our survey we reached women from rural areas but in the interview phase rural women were not included as they were not willing to proceed. Despite keeping the socio-economical conditions of Bangladeshi women in mind, the prototype model has been made with limited data hence it does not have complete functionality for complete set of KPI(Key Performance testing) testing and may generate potential inaccuracies of component pathways if the design material

become too complex.

10.3 Future work

Our plan for the future is to work on our proposed framework, making it a full functional website that can reach women from urban to rural areas to address our identified gaps in the research. Additionally, further work should also focus on engaging more with experts and policymakers which can provide a more understanding of the structural and policy related disparities.

10.4 Conclusion

This research investigates the cybersecurity awareness knowledge among Bangladeshi women through a holistic exploration. Our work is distincted by inclusion of a wide range of women from diverse demographics. This study helps to fill the existing research gap by offering insights into women focused cybersecurity awareness knowledge evaluation. By examining cybersecurity awareness and practice across important aspects of cybersecurity, our study identifies cybersecurity awareness knowledge among Bangladeshi women. Our findings highlight that women's exposure to cyber threats is not solely a consequence of insufficient awareness but also influenced by behavioral patterns and situational vulnerabilities. We discovered the most frequent risk and threat faced by women and the underlying cause of these threats. Additionally, we assessed women's response to security warnings and identified action-inaction to their experienced cyber threats. Moreover, our research addresses women's perspective on security and privacy features as well as policies across their digital usage and experience. Furthermore, we uncover possible barriers of women that hinder them from reporting cybersecurity threats. Finally, based on our research findings we propose a framework to overcome the knowledge disparities. Our research outcome hopes to strengthen cybersecurity protection while providing pragmatic solutions to improve awareness programmes, educational initiatives and policies in Bangladesh.

References

[1] L. A. Goodman, "Snowball sampling," *The annals of mathematical statistics*, pp. 148–170, 1961.

[2] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," *The journal of psychology*, vol. 91, no. 1, pp. 93–114, 1975.

[3] T. K. Landauer, "Research methods in human-computer interaction," in *Handbook of human-computer interaction*, Elsevier, 1988, pp. 905–928.

[4] I. Ajzen, "The theory of planned behavior," *Organizational behavior and human decision processes*, vol. 50, no. 2, pp. 179–211, 1991.

[5] R. Singh, N. S. Mangat, R. Singh, and N. S. Mangat, "Stratified sampling," *Elements of survey sampling*, pp. 102–144, 1996.

[6] J. M. Carroll, "Human-computer interaction: Psychology as a science of design," *Annual review of psychology*, vol. 48, no. 1, pp. 61–83, 1997.

[7] M. Zviran and W. J. Haga, "Password security: An empirical study," *Journal of management information systems*, vol. 15, no. 4, pp. 161–185, 1999.

[8] A. Parasuraman, "Technology readiness index (tri) a multiple-item scale to measure readiness to embrace new technologies," *Journal of service research*, vol. 2, no. 4, pp. 307–320, 2000.

[9] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security," *BT technology journal*, vol. 19, no. 3, pp. 122–131, 2001.

[10] P. Bocij and L. McFarlane, "Online harassment: Towards a definition of cyberstalking," *Prison Service Journal*, pp. 31–38, 2002.

[11] N. Nicholson, E. Soane, M. Fenton-O'Creevy, and P. Willman, "Personality and domain-specific risk taking," *Journal of Risk Research*, vol. 8, no. 2, pp. 157–176, 2005.

[12] D. Rickwood, F. P. Deane, C. J. Wilson, and J. Ciarrochi, "Young people's help-seeking for mental health problems," *Australian e-journal for the Advancement of Mental health*, vol. 4, no. 3, pp. 218–251, 2005.

[13] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. C. Mitchell, "Stronger password authentication using browser extensions.," in *USENIX Security Symposium*, Baltimore, MD, USA, vol. 17, 2005, p. 32.

[14] S. Gaw and E. W. Felten, "Password management strategies for online accounts," in *Proceedings of the second symposium on Usable privacy and security*, 2006, pp. 44–55.

[15] D. Florencio and C. Herley, "A large-scale study of web password habits," in *Proceedings of the 16th international conference on World Wide Web*, 2007, pp. 657–666.

[16] F. Dehue, C. Bolman, and T. Völlink, "Cyberbullying: Youngsters' experiences and parental perception," *CyberPsychology & Behavior*, vol. 11, no. 2, pp. 217–223, 2008.

[17] C. IT, *Cyber security and ethical hacking course*, Accessed: 2025-01-31, 2008. [Online]. Available: https://www.creativeitinstitute.com/courses/cyber-security-ethical-hacking.

[18] C. Riessman, *Narrative methods for the human sciences*. Sage, 2008.

[19] D. Halder and J. Karuppannan, "Cyber socializing and victimization of women," *The Journal on Victimization*, vol. 12, no. 3, pp. 5–26, 2009.

[20] S. Bagchi-Sen, H. R. Rao, S. J. Upadhyaya, and S. Chai, "Women in cybersecurity: A study of career advancement," *IT professional*, vol. 12, no. 1, pp. 24–31, 2010.

[21] R. Kainda, I. Flechais, and A. Roscoe, "Security and usability: Analysis and evaluation," in *2010 international conference on availability, reliability and security*, IEEE, 2010, pp. 275–282.

[22] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching johnny not to fall for phish," *ACM Transactions on Internet Technology (TOIT)*, vol. 10, no. 2, pp. 1–31, 2010.

[23] R. Shay, S. Komanduri, P. G. Kelley, *et al.*, "Encountering stronger password requirements: User attitudes and behaviors," in *Proceedings of the sixth symposium on usable privacy and security*, 2010, pp. 1–20.

[24] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions," in *Proceedings of the SIGCHI conference on human factors in computing systems*, 2010, pp. 373–382.

[25] R. Wash, "Folk models of home computer security," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, 2010, pp. 1–16.

[26] M. Blythe, H. Petrie, and J. A. Clark, "F for fake: Four studies on how we fall for phish," in *Proceedings of the SIGCHI conference on human factors in computing systems*, 2011, pp. 3469–3478.

[27] H. Steyerl, "Digital debris: Spam and scam.," *October*, no. 138, 2011.

[28] J. Cowie, *Climate change: biological and human aspects*. Cambridge University Press, 2012.

[29] A. Darwish, A. El Zarka, and F. Aloul, "Towards understanding phishing victims' profile," in *2012 International Conference on Computer Systems and Industrial Informatics*, IEEE, 2012, pp. 1–5.

[30] T. Halevi, J. Lewis, and N. Memon, "A pilot study of cyber security and privacy related behavior and personality traits," in *Proceedings of the 22nd international conference on world wide web*, 2013, pp. 737–744.

[31] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram, "Phishing for the truth: A scenario-based experiment of users' behavioural response to emails," in *Security and Privacy Protection in Information Processing Systems: 28th IFIP TC 11 International Conference, SEC 2013, Auckland, New Zealand, July 8-10, 2013. Proceedings 28*, Springer, 2013, pp. 366–378.

[32] D. Charoen, "Password security," *International Journal of Security (IJS)*, vol. 8, no. 1, pp. 1–14, 2014.

[33] B. C. Institute, *Bangladesh cyber institute*, Accessed: 2025-01-31, 2014. [Online]. Available: https://cyberinstitutebd.com/.

[34] N. Kortjan and R. Von Solms, "A conceptual framework for cyber-security awareness and education in sa," *South African Computer Journal*, vol. 52, no. 1, pp. 29–41, 2014.

[35] M. N. Nabi and M. T. Islam, "Cyber security in the globalized world: Challenges for bangladesh," *Economic and Social Development: Book of Proceedings*, p. 32, 2014.

[36] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the human aspects of information security questionnaire (hais-q)," *Computers & security*, vol. 42, pp. 165–176, 2014.

[37] T. Saha and A. Srivastava, "Indian women at risk in the cyber space: A conceptual model of reasons of victimization.," *International Journal of Cyber Criminology*, vol. 8, no. 1, 2014.

[38] E. O. Yeboah-Boateng and P. M. Amanor, "Phishing, smishing & vishing: An assessment of threats against mobile devices," *Journal of Emerging Trends in Computing and Information Sciences*, vol. 5, no. 4, pp. 297–307, 2014.

[39] B. B. Anderson, C. B. Kirwan, J. L. Jenkins, D. Eargle, S. Howard, and A. Vance, "How polymorphic warnings reduce habituation in the brain: Insights from an fmri study," in *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, 2015, pp. 2883–2892.

[40] B. e-Govt CIRT, *Incident reporting - cirt*, Accessed: 2025-01-31, 2015. [Online]. Available: https://www.cirt.gov.bd/incident-reporting/.

[41] S. D. Pawlowski and Y. Jung, "Social representations of cybersecurity by university students and implications for instructional design," *Journal of Information Systems Education*, vol. 26, no. 4, pp. 281–294, 2015.

[42] T. Petsas, G. Tsirantonakis, E. Athanasopoulos, and S. Ioannidis, "Two-factor authentication: Is the world ready? quantifying 2fa adoption," in *Proceedings of the eighth european workshop on system security*, 2015, pp. 1–7.

[43] K. Wozencroft, M. Campbell, A. Orel, M. Kimpton, and E. W. Leong, "University students' intentions to report cyberbullying," *Australian journal of educational and developmental psychology*, vol. 15, pp. 1–12, 2015.

[44] C. Laybats and L. Tredinnick, *Information security*, 2016.

[45] J. Muhirwe and N. White, "Cybersecurity awareness and practice of next generation corporate technology users," *Issues in Information Systems*, vol. 17, no. 2, 2016.

[46] N. Ahmed, U. Kulsum, I. B. Azad, A. Z. Momtaz, M. E. Haque, and M. S. Rahman, "Cybersecurity awareness survey: An analysis from bangladesh perspective," in *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, IEEE, 2017, pp. 788–791.

[47] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: State of the art and future challenges," *Neural Computing and Applications*, vol. 28, pp. 3629–3654, 2017.

[48] D. Huynh, P. Luong, H. Iida, and R. Beuran, "Design and evaluation of a cybersecurity awareness training game," in *Entertainment Computing–ICEC 2017: 16th IFIP TC 14 International Conference, Tsukuba City, Japan, September 18-21, 2017, Proceedings 16*, Springer, 2017, pp. 183–188.

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

[50] M. A. Bujang, E. D. Omar, and N. A. Baharum, "A review on sample size determination for cronbach's alpha test: A simple guide for researchers," *The Malaysian journal of medical sciences: MJMS*, vol. 25, no. 6, p. 85, 2018.

[51] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," *computers & security*, vol. 73, pp. 345–358, 2018.

[52] N. Kabir, "Cyber crime a new form of violence against women: From the case study of bangladesh," *Available at SSRN 3153467*, 2018.

[53] F. Khalid, M. Y. Daud, M. J. A. Rahman, and M. K. M. Nasir, "An investigation of university students' awareness on cyber security," *International Journal of Engineering & Technology*, vol. 7, no. 421, pp. 11–14, 2018.

[54] S. Kundu, K. A. Islam, T. T. Jui, S. Rafi, M. A. Hossain, and I. H. Chowdhury, "Cyber crime trend in bangladesh, an analysis and ways out to combat the threat," in *2018 20th International Conference on Advanced Communication Technology (ICACT)*, IEEE, 2018, pp. 474–480.

[55] S. Rezayi, V. Balakrishnan, S. Arabnia, and H. R. Arabnia, "Fake news and cyberbullying in the modern era," in *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*, IEEE, 2018, pp. 7–12.

[56] N. Sambasivan, G. Checkley, A. Batool, *et al.*, "" privacy is not for me, it's for those rich women": Performative privacy practices on mobile phones by women in south asia," in *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 2018, pp. 127–142.

[57] P. Seemma, S. Nandhini, and M. Sowmiya, "Overview of cyber security," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 7, no. 11, pp. 125–128, 2018.

[58] N. I. of Standards and T. (NIST), *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy*, https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final, 2018.

[59] S. Sultana, F. Guimbretière, P. Sengers, and N. Dell, "Design within a patriarchal society: Opportunities and challenges in designing for rural women in bangladesh," in *Proceedings of the 2018 CHI conference on human factors in computing systems*, 2018, pp. 1–13.

[60] V. Valipe, "Impact of phishing on businesses: User awareness and response triggers to phishing emails," M.S. thesis, University of Nebraska at Omaha, 2018.

[61] N. Ahmed, M. R. Islam, U. Kulsum, M. R. Islam, M. E. Haque, and M. S. Rahman, "Demographic factors of cybersecurity awareness in bangladesh," in *2019 5th International Conference on Advances in Electrical Engineering (ICAEE)*, IEEE, 2019, pp. 685–690.

[62] R. Anderson, C. Barton, R. Böhme, *et al.*, "Measuring the changing cost of cybercrime," in *The 18th Annual Workshop on the Economics of Information Security (WEIS 2019)*, 2019.

[63] A. Haque, "Need for critical cyber defence, security strategy and privacy policy in bangladesh-hype or reality?" *arXiv preprint arXiv:1906.01285*, 2019.

[64] J. Jeong, J. Mihelcic, G. Oliver, and C. Rudolph, "Towards an improved understanding of human factors in cybersecurity," in *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, IEEE, 2019, pp. 338–345.

[65] Ö. A. Aslan and R. Samet, "A comprehensive review on malware detection approaches," *IEEE access*, vol. 8, pp. 6249–6271, 2020.

[66] S. Autio, "The impact of social media on consumer purchasing behavior," 2020.

[67] C. Bangla, *Cyber bangla academy*, Accessed: 2025-01-31, 2020. [Online]. Available: https://academy.cyberbangla.org/.

[68] S. T. Haque, M. R. Haque, S. Nandy, *et al.*, "Privacy vulnerabilities in public digital service centers in dhaka, bangladesh," in *Proceedings of the 2020 International Conference on Information and Communication Technologies and Development*, 2020, pp. 1–12.

[69] S. A. Kabir, "Many women in bangladesh create online businesses during pandemic," *The Financial Express*, 2020. [Online]. Available: https://thefinancial%20express.com.bd/trade/many-women-in-bangladesh-create-online-businesses-during-pandemic-1609255446.

[70] S. M. Kennison and E. Chan-Tin, "Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors," *Frontiers in Psychology*, vol. 11, p. 546 546, 2020.

[71] Z. Zulkifli, N. N. A. Molok, N. H. Abd Rahim, and S. Talib, "Cyber security awareness among secondary school students in malaysia," *Journal of information systems and digital technologies*, vol. 2, no. 2, pp. 28–41, 2020.

[72] O. A. Adeoye-Olatunde and N. L. Olenik, "Research and scholarly methods: Semi-structured interviews," *Journal of the american college of clinical pharmacy*, vol. 4, no. 10, pp. 1358–1367, 2021.

[73] A. Al Habsi, M. Butler, A. Percy, and S. Sezer, "Blackmail on social media: What do we know and what remains unknown?" *Security Journal*, vol. 34, pp. 525–540, 2021.

[74] S. Baadel, F. Thabtah, and J. Lu, "Cybersecurity awareness: A critical analysis of education and law enforcement methods," *Informatica*, vol. 45, no. 3, 2021.

[75] V. Braun and V. Clarke, "To saturate or not to saturate? questioning data saturation as a useful concept for thematic analysis and sample-size rationales," *Qualitative research in sport, exercise and health*, vol. 13, no. 2, pp. 201–216, 2021.

[76] M. Grobler, R. Gaire, and S. Nepal, "User, usage and usability: Redefining human centric cyber security," *Frontiers in big Data*, vol. 4, p. 583 723, 2021.

[77] A. Maraj, C. Sutherland, and W. Butler, "Studying the challenges and factors encouraging girls in cybersecurity: A case study," in *ECCWS 2021 20th European Conference on Cyber Warfare and Security*, Academic Conferences Inter Ltd, 2021, p. 269.

[78] T. D. Nguyen, M.-H. Shih, D. Srivastava, S. Tirthapura, and B. Xu, "Stratified random sampling from streaming and stored data," *Distributed and Parallel Databases*, vol. 39, pp. 665–710, 2021.

[79] J. R. Nurse, "Cybersecurity awareness," in *Encyclopedia of Cryptography, Security and Privacy*, Springer, 2021, pp. 1–4.

[80] D. Papatsaroucha, Y. Nikoloudakis, I. Kefaloukos, E. Pallis, and E. K. Markakis, "A survey on human and personality vulnerability assessment in cyber-security: Challenges, approaches, and open issues," *arXiv preprint arXiv:2106.09986*, 2021.

[81] R. J. Rony, N. Saliheen, and N. Ahmed, "Cybercrime experiences, handling and practices: A reality check in the perspective of urban bangladesh," *Handling and Practices: A Reality Check in the Perspective of Urban Bangladesh (July 13, 2021)*, 2021.

[82] R. J. Rony, N. Saliheen, and N. Ahmed, "Cybercrime experiences, handling and practices: A reality check in the perspective of urban bangladesh," *Handling and Practices: A Reality Check in the Perspective of Urban Bangladesh (July 13, 2021)*, 2021.

[83] T. Daengsi, P. Pornpongtechavanich, and P. Wuttidittachotti, "Cybersecurity awareness enhancement: A study of the effects of age and gender of thai employees associated with phishing attacks," *Education and Information Technologies*, pp. 1–24, 2022.

[84] M. E. Erendor and M. Yildirim, "Cybersecurity awareness in online education: A case study analysis," *Ieee Access*, vol. 10, pp. 52 319–52 335, 2022.

[85] J. Golzar, S. Noor, and O. Tajik, "Convenience sampling," *International Journal of Education & Language Studies*, vol. 1, no. 2, pp. 72–77, 2022.

[86] M. J. Hossain, "User privacy & security in internet: A concern for bangladesh," Ph.D. dissertation, Noakhali Science and Technology University, 2022.

[87] H. Hussain, "Password security: Best practices and management strategies," *Available at SSRN 4136333*, 2022.

[88] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: A comparative study," *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 82–97, 2022.

[89] I. Advisory and C. Ltd., *Insights from "strengthening cybersecurity for facebook commerce businesses" webinar*, Accessed: 2025-01-31, 2023. [Online]. Available: https://inspira-bd.com/https-www-facebook-com-inspiraacl-videos-1395202618096170-mibextidyxdkmj/.

[90] Y. Hong, M.-J. Kim, and T. Roh, "Mitigating the impact of work overload on cybersecurity behavior: The moderating influence of corporate ethics—a mediated moderation analysis," *Sustainability*, vol. 15, no. 19, p. 14 327, 2023.

[91] R. Kant, "Cyber-security awareness in india: How much students of higher education are aware?" *Education Sciences & Psychology*, vol. 67, no. 2, 2023.

[92] N. A. Rakha, "Cyber law: Safeguarding digital spaces in uzbekistan," *International Journal of Cyber Law*, vol. 1, no. 5, 2023.

[93] K. Renaud and M. Dupuis, "Cybersecurity insights gleaned from world religions," *Computers & Security*, vol. 132, p. 103 326, 2023.

[94] A. S. Sikder, "Unveiling the human aspect of cybersecurity: A holistic examination of employee behavior and its significance in safeguarding organizational security within the context of bangladesh: Human aspect of cybersecurity.," *International Journal of Imminent Science & Technology*, vol. 1, no. 1, pp. 199–215, 2023.

[95] T. D. Star, "Smart bangladesh, unsmart cybersecurity measures," *The Daily Star*, 2023. [Online]. Available: https://www.thedailystar.net/opinion/views/closer-look/news/smart-bangladesh-unsmart-cybersecurity-measures-3439906.

[96] B. Ahamed, M. R. H. Polas, A. I. Kabir, *et al.*, "Empowering students for cybersecurity awareness management in the emerging digital era: The role of cybersecurity attitude in the 4.0 industrial revolution era," *SAGE Open*, vol. 14, no. 1, p. 21 582 440 241 228 920, 2024.

[97] S. Al Kandy, "Evolution and challenges of cyber law in the digital era: Case studies in developing countries," *ILAW; International Journal Assulta of Law Review*, vol. 1, no. 1, pp. 1–10, 2024.

[98] Y. Asiry, "Closing the gap: Boosting women's representation in cybersecurity leadership," *Journal of Information Security*, vol. 15, no. 01, pp. 15–23, 2024.

[99] V. Braun and V. Clarke, "Thematic analysis," in *Encyclopedia of quality of life and well-being research*, Springer, 2024, pp. 7187–7193.

[100] H. Correspondent, "Hackers spreading malware via kids' gaming websites," *Hindustan Times*, 2024. [Online]. Available: https://www.hindustantimes.com/business/hackers-spreading-malware-via-kids-gaming-websites/story-CWm9w6hgSJHLR4TIEbh3DO.html.

[101] F. T. Johora, M. S. I. Khan, E. Kanon, M. A. T. Rony, M. Zubair, and I. H. Sarker, "A data-driven predictive analysis on cyber security threats with key risk factors," *arXiv preprint arXiv:2404.00068*, 2024.

[102] J. Koziol. "Cybersecurity awareness: What it is and how to start." Accessed: 04 June 2024, Forbes. (2024), [Online]. Available: https://www.forbes.com/advisor/business/what-is-cybersecurity-awareness/.

[103] C. Mittal, "An empirical study on cybersecurity awareness, cybersecurity concern, and vulnerability to cyber-attacks," *Valley International Journal Digital Library*, pp. 1144–1158, 2024.

[104] S. Busetti and F. M. Scanni, "Evaluating incident reporting in cybersecurity. from threat detection to policy learning," *Government Information Quarterly*, vol. 42, no. 1, p. 102 000, 2025.

[105] F. Ferdous, M. H. Nahid, and N. Farhana, "Cyber security awareness among generation z in bangladesh,"

[106] *How a spelling mistake stopped hackers stealing $1bn in a bank heist — independent.co.uk*, https://www.independent.co.uk/news/world/asia/spelling-mistake-stops-hackers-stealing-1-billion-in-bangladesh-bank-heist-a6924971.html, [Accessed 20-10-2024].

[107] M. T. Islam, "Investigating factors influencing the adoption of information security awareness of the individual users: An empirical study in bangladesh,"

[108] M. A. Uddin, A. Z. Supti, A. Asgar, and M. S. Mridha, "Cyber security awareness (csa) and cyber crime in bangladesh: A statistical modeling approach,"

Appendix A

Appendix

A.1 Survey Questions

The following section consists of the survey questions for quantitive data collection.

- 1. Which of the following describes your current status?
- 2. What is your age?
  - **Demographics**
    - **Working Professional**
      - 1. What is your status?
      - 2. How would you identify the area your employment?
      - 3. How would you identify the area you reside?
      - 4. How many years have you been using digital devices (e.g., computers, smartphones, tablets)
      - 5. How much time do you spend on your digital device daily?
    - **University Student**
      - 1. What is your academic status?
      - 2. How would you identify the field of your study?
      - 3. How would you identify the area you live?
      - 4. How many years have you been using digital devices (e.g., computers, smartphones, tablets)?
      - 5. How much time do you spend on your digital device daily?
    - **High-school Student**
      - 1. What is your current class or grade level of education?
      - 2. How would you identify the field of your study?
      - 3. How would you identify the area you live?
      - 4. How many years have you been using digital devices (e.g., computers, smartphones, tablets)?
      - 5. How much time do you spend on your digital device daily?
- **Password security**

- 1. For multiple accounts (personal /university /work-related), do you have the tendency to use the same password?
- 2. Do you use personal information (e.g., name, birthdate, favorite singer etc.) while creating your passwords?
- 3. How consistent are you activating two-factor authentication (2FA) to secure your accounts? (2FA is a Security method that requires two form of identification to log in to your accounts)
- 4. To what extent, you feel your passwords are strong, safe and secure enough?
- 5. Which method do you generally follow to keep your passwords safe? (If "Other," please specify)

- **Information security**
  - 1. Do you know "Phishing"?
  - 2. Which one do you think is an example of phishing?
  - 3. Have you attended any cyber security awareness training /seminar /workshop sessions at your school/university/ workplace?
  - 3. Have you attended any cyber security awareness training /seminar /workshop sessions at your school/university/ workplace?

- **Device Privacy**
  - 1. Do you share your smartphone with others? (e.g Family, Friends or anyone known or unknown to you)
  - 2. Do you review or adjust the permissions granted to apps after installation?
  - 3. Are you aware of the risks of using public Wi-Fi?
  - 4. How do you protect your device from unauthorized access?

- **Incident reporting**
  - 1. Have you ever faced and reported a cyberbullying incident?
  - 2. In case your password, device, social media account, or personal information were hacked or leaked , do you know the steps to secure them and what actions would you take?
  - 3. Are you confident in your ability to handle cyber attacks?

- **Malware Detection**
  - 1. How would you know if your device is infected by malware?"
  - 2. Are you cautious about downloading resources like academic papers/games/movies from unknown sources?
  - 3. Do you have any experience in the usage of malware detection tools?
  - 4. How frequently do you use anti-malware software to scan or protect your devices?

A.2 Interview Questions

The following section consists of the interview questions for qualitative data collection.

- **Demographics**
  - 1. Can you please tell how old are you?
  - 2. What is your current academic / job status?
  - 3. Can you share a bit about your background in terms of economic status?
  - 4. Can you please tell me what your residence area is ?
  - 5. How many years have you been using digital devices ? (e.g., computers, smartphones, tablets)
- **Cyber security Awareness Knowledge**
  - 1. What do you understand about the term "Cybersecurity awareness"?
  - 2. How do you know about this term? (training, textbook, social media, television and etc
- **Device Usage Practice**
  - 1. Could you please tell us what kind of device you use? (smartphone ,feature phone, computer and tab
  - 2. How much time do you spend on your digital device daily?
  - 3. Do you think your activity on your device or internet is always safe?
    - a. If yes, why, how?
    - b. If not why not, for which reason, describe the reason.

    In which purpose do you mostly use the internet for academic/knowledge or entertainment purposes?
  - 4. Do you use your personal digital device or share with any of your family members?
    - a. If shared then, do you have a separate account in the shared phone or not?
    - b. Do you feel comfortable while sharing, if not comfortable why not?
- **Security threats and risky Experience**
  - 1. Have you ever gone through a situation while using your digital device or internet where you encountered a risky situation ? (in your personal life, work life)
    - a. If yes, what was that ?
  - 2. Can you describe to me what was the main reason that caused you to take that risk ?

- 3. After you encountered that security threat, what do you feel was lacking in your capability that led you to this risk?
- 4. As for this situation you faced, have you taken any action to prevent it or just ignored it?
  * a. If yes what was that prevention or precaution methods?
  * b. If there is no report or prevention steps, why and what reason behind it?
- 5. If you face that risk again in future how would you plan to handle it?
- 6. Do you think there are any specific online threats that mostly target women, and if so, what are they?
- 7. Has your social media account ever got hacked or you noticed any suspicious activity on it?
  * a. What do you think is the main reason behind the hacking of any social media e.g., Facebook, WhatsApp and etc?
- **Privacy and Security Concern**
  * 1. When you think about digital privacy and security, what do you understand about these?
  * 2. To what extent do you believe revealing your personal information is no longer safe and secure online?
  * 3. Which privacy and security features of any websites or apps have, that are mostly trustworthy and not trust worthy at all to you ?
  * 4. Can you tell me about a situation when you saw an online security or privacy concern warning yet you chose to ignore it ? What were the reasons that pushed you to make this choice?
- **Suggestions and Goals**
  * 1. What important steps and advice would you suggest to other women so that they may protect themselves and be more careful online?
    Educational Initiatives
  * 2. What kind of educational resources or training would be most effective for women to improve their cybersecurity awareness?
    Policy and Structural Suggestions
  * 3. What specific cybersecurity policies, features or improvements would make you feel more safer when browsing the internet?
  * 3. What kind of learning and essential resource would be most useful to improve your knowledge of cybersecurity?
  * 4. Do you think that a website with networking, forums, interactive learning (videos, quizzes, short videos) and essential resources would be enough to improve cybersecurity understanding for you and for women of all demographics?

A.3 Model Features

The following consists of the pictures of model features:

- **Video Tutorials**: Video tutorials serve as the fundamental element of the website since they provide cybersecurity education in both English and Bengali language The video tutorials of the website present information on Password Security, Information Security, Device Privacy, Incident Reporting and Malware Detection

Figure A.1: Video tutorials

- **Events, workshops and seminar**: The platform functions as an online bulletin board to promote upcoming cybersecurity education activities which take place throughout the world and across local communities. Figure available at A.2.

- **Cyber Incident Updates**: The section contains recent reports and case examples regarding genuine cyber incidents along with details about data breaches followed by descriptions of phishing attacks and malware outbreaks which is provided by our users whoever has experienced and witnessed it. Figure A.3 visualize the cyber incident updates feature.

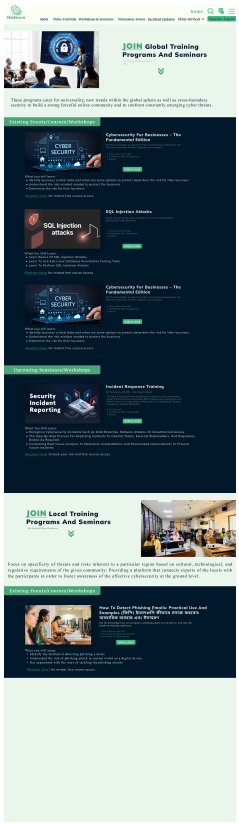

Figure A.2: Events, workshops and seminar

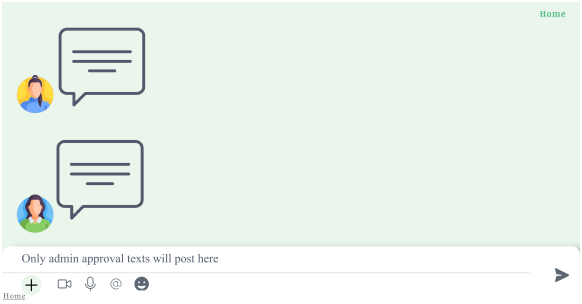

Figure A.3: Cyber incident updates

- **Discussion Forum**: Users can participate in the discussion forum which serves as an interactive environment where they can safely exchange dialogues about cyber events or best practices with their peers. Figure available at A.4

Figure A.4: Discussion forum

- **Testing tools**: Among its features this platform shares direct links to multiple safe cybersecurity testing instruments including phishing link verification tools and malware detectors which users can access at no cost. Figure available at A.5

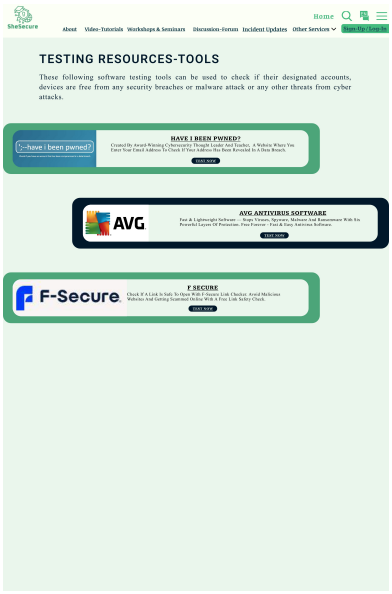

Figure A.5: Testing tools

- **Expert Consultation**: Users of this platform can reach out to security consultants with experience through the expert consultation feature to solve particular issues or address questions. Figure available at A.6

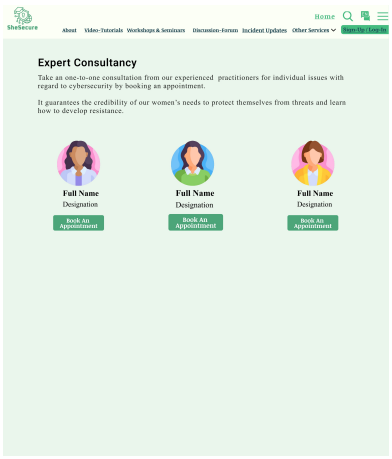

Figure A.6: Expert consultation

- **Quizzes**: Users can assess their cybersecurity knowledge through the quizzes which create evaluation opportunities for different subjects. Figure A.7 represents the quizzes feature.

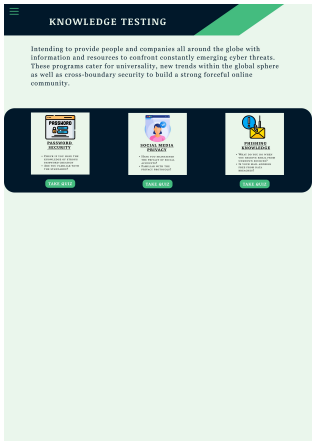

Figure A.7: Quizzes

- **News and Articles**: Users can access the latest updates from the cybersecurity world through this section which covers new security threats as well as technological advancements and profiles of women in cybersecurity work. Figure A.8 shows the feature News and Articles.

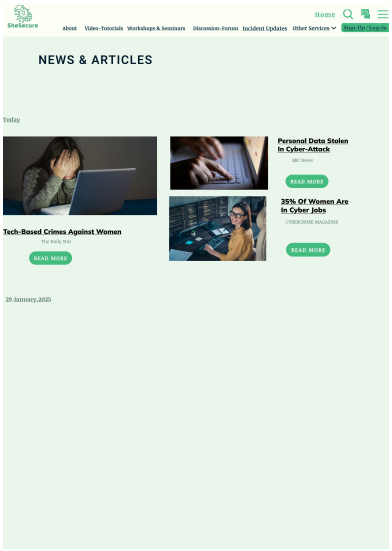

Figure A.8: News and article

- **Help Desk**: This feature enables our users to resolve technical issues or difficulties and request website maintenance or ask questions about website capabilities. Figure A.9 represents the the Help Desk feature.

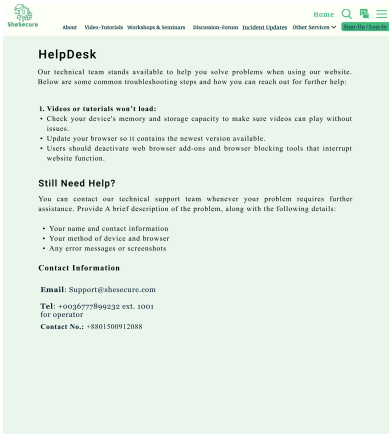

Figure A.9: Help desk

A.4 Hypothesis result

Hypothesis result in Table A.1

A.5 Codebook

Thematic analysis codebook in Table A.2

Narrative analysis codebook in Table A.3

Hypothesis	**High School Students**	**University Students**	**Working Women**
H1: Women who reuse passwords across accounts might be less likely to consistently use 2FA.	Not Supported	Not Supported	Not Supported
H2: The confidence in women's ability to handle cyber-attacks correlates with reporting cyberbullying incidents.	• When Level of confidence is 5: – Probability of reporting: 22.78% • When Level of confidence is 0: – Probability of reporting: 12.62%	• When Level of confidence is 5: – Probability of reporting: 65.65% • When Level of confidence is 0: – Probability of reporting: 30.02%	• When Level of confidence is 5: – Probability of reporting: 53.86% • When Level of confidence is 0: – Probability of reporting: 17.88%
H3: Women's field of study and employment correlates with their ability to identify phishing examples and malware detection on their device.	Not Supported	Not Supported	Not Supported

Table A.1: Summary of results for each hypothesis across three groups

Category	Code	Description
Cybersecurity Awareness	Devices safety	Awareness of keeping devices secure from hack and scam
	Password Management	Managing passwords and regularly changing them.
	Data Privacy Awareness	Understanding how to keep personal data secure and prevent data leaks.
	Awareness through Experience	Awareness gained by online risks like scams, phishing and hacks.
Device Usage	Device and login security	Using their own device and logout from others, restrict sharing password.
	Uncertain safety	Feeling of being under surveillance and threat .
	Impulsive decision	Clicking in suspicious link, lead to security risk.
Security Threats	Hacking	Personal accounts got compromised, hacked, or identity theft, accessed without permission.
	Phishing & Vishing	Security threats through phone call & messages.
	Fraud & Scam	Scams that leads to financial loss.
	Cyber harrasment	Facing inappropriate message .
	Impersonation & Catfishing	Exposing fake identities to deceive and manipulate.
Women centric online threats	stalking and troll	Stalking and troll makes insecure.
	AI Misuse	Making deepfake and fake photos
	Blackmail	Using social media accounts to blackmail or to disturb women.
Awareness & Education	Awareness education	education through textbooks, academic courses and seminars.
	Social Media & Online Learning	cybersecurity knowledge through social media,influencer and online resources.
	Family and Peer Learning	Learning about cybersecurity through family members friends and educational institution.
Online Safety Precautions	Profile Privacy	Keeping personal information private.
	No Stranger Interaction	Not responding on unknown people's message.
	Privacy Settings	Using privacy settings and security measures such as 2FA.
	Avoiding Suspicious links	Not clicking on untrustworthy links

Table A.2: Thematic analysis codebook

Category	Code	Description
Human behaviour	Overtrust/Blind faith	Believing on people word and get influence easily.
	Convenience over security	Choosing easy way leads to vulnerable or unsafe in digital world.
	Unconscious/Negligence	Not being enough caucious to security warnings
Situational factor	insufficient awareness	deprived from having basic knowledge of cybersecurity.
	weak security practice	Not using security tools and feature
	Poor privacy control	Sharing OTP and credential infronmation with others.
Response to security warnings	Dependency	Exsessive dependency on online resourse due to cost and necessity
	Desensitisation	Being habituated with dismissing security warnings
	Dismissal of pop up	Ignoring the pop up warning for being annoyed
Response to threats	Ignoring	Not knowing what to and fear of parental anger
	2FA use	Started using 2FA after encounting with risk.
	Complained to authority	Complain to respective platform but did not get response.
Trustworthy/Untrusworthy	Facebook	Safe-profile guard, unsafe-photo download
	Instagram	safe- parental supervision, unsafe-SSO.
	WhatsApp	safe-QR code security, unsafe-open group invitition

Table A.3: Narrative analysis codebook