# CyberGuard Chronicles: Design, Implementation, and Assessment of a Game-Based Platform for Cybersecurity Awareness in Bangladesh

by

Fatema Khanom
23241127
Sumaya Hasan Prokrity
21201455
Mir Saiyara Iffat
21201753
Tawkir Arifin
21201597
Shamrat Neero
21201343

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
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:**

Fatema Khanom
23241127

Sumaya Hasan Prokrity
21201455

Mir Saiyara Iffat
21201753

Tawkir Arifin
21201597

Shamrat Neero
21201343

# Approval

The thesis/project titled "CyberGuard Chronicles: Design, Implementation and Assessment of a Game-Based Platform for Cybersecurity Awareness in Bangladesh" submitted by

1. Fatema Khanom (23241127)
2. Sumaya Hasan Prokrity(21201455)
3. Mir Saiyara Iffat (21201753)
4. Tawkir Arifin (21201597)
5. Shamrat Neeero (21201343)

Of Summer, 2025 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on October 10, 2025.

**Examining Committee:**

Supervisor:
(Member)

Dr. Farida Chowdhury
Professor
Department of Computer Science and Engineering
Brac University

Thesis Coordinator:
(Sign)

Md. Golam Rabiul Alam, PhD
Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)

Sadia Hamid Kazi, PhD
Chairperson and Associate Professor
Department of Computer Science and Engineering
Brac University

# Ethics Statement

This research, titled **"CyberGuard Chronicles: Design, Implementation, and Assessment of a Game-Based Platform for Cybersecurity Awareness in Bangladesh"** was conducted in accordance with ethical guidelines to ensure the rights, dignity, and confidentiality of all participants. Participants were fully informed about the study's objectives, procedures, potential risks, and their rights before their involvement. Informed consent was obtained both orally and in written form, ensuring voluntary participation. Additionally, for younger participants (ages 10–16), consent was obtained from their parents or guardians. Participants were given the freedom to withdraw from the study at any stage without facing any consequences.

To maintain confidentiality, all personal identifiers were anonymized, and data were securely stored with restricted access to authorized researchers only. The research adhered to national and international ethical guidelines, ensuring compliance with data protection and research integrity principles. This study was conducted with the utmost consideration for ethical standards, ensuring transparency, fairness, and participant well-being throughout the research process.

# Abstract

The online world is being bombarded with information that users need to be aware of, and in developing nations such as Bangladesh, high levels of social media exposure can become deadly and pose online safety threats to users with little experience in internet safety and navigation. In this context, target age groups of young internet users (10-16 years) and older age groups (45+ years) can be vulnerable to internet security threats, as they have frequent presence on the internet and have a limited understanding of it. This thesis uses a human-centred design (HCD) approach to design, assess, and implement a gamified platform for basic cybersecurity training and enhance the human-computer interaction for safer usage and navigation on the internet. The platform was developed using the Bangladeshi context in particular. To identify the risks and potential hazards, initially, semi-structured interviews (n=63) were held with the selected age groups. Moreover, the results from the interviews were used to identify the loopholes and the preferred method to combat the situation. The interviews were used to highlight the major risky areas, such as safe usage of passwords or password hygiene (PH), potential hazards of phishing, etc. The result also backed up the gamified approach with a major acceptance from the young participants. However, 68.57% of older participants preferred secondary methods like classroom or seminars. Based on these findings, a role-playing game (RPG) was developed in Unity engine to implement the gamification technology and help simulate and navigate real cyber threats. To make the approach more concrete, the RPG was then compared to a traditional lesson in a controlled study environment(n=96), in the case of the young participants' age group, as the older participants were reluctant to the gamified intervention. The results concluded that gamified technology had better learning gains and higher engagement for the young participants. The theoretical contributions of this work include a HCD-informed needs assessment for cybersecurity education at a foundational level in Bangladesh, a context-informed RPG solution, and empirical proof that game-based learning can achieve better results for younger learners. Moreover, our work suggests further implications in the national curriculum to enhance cybersecurity awareness and promote best practices.

**Keywords:** Cyber security awareness for developing countries; Role Play Games (RPG); Gamification; Cybersecurity framework; Gamified E-learning; Controlled Study; Human-Centred Design

# Table of Contents

# List of Figures

# List of Tables

# Nomenclature

The next list describes several symbols & abbreviation that will be later used within the body of the document

$HUD$ Heads Up Display

$RPG$ Role Play game

# Chapter 1

# Introduction

The cyber world is a large connectivity of computers and is a very interconnected network, but there exists a growing threat along with it in the personal, home, or office network. With the skyrocketing of internet use, cyber readiness, such as identity theft and trading of stolen identities, is at an alarming rate. Compared to Western countries, Bangladesh, with internet access starting every year since 1996, has a much lower level of cybersecurity awareness [15]. This lack of awareness is a huge threat to older persons (45+) as well as youngsters (10-16 years old), who rely heavily on the internet without often having the necessary knowledge to protect themselves.

In this context, children and adolescents (worldwide and in Somalia: it is 10-16 years) and elderly persons (45+ years) are especially vulnerable to internet security threats because they are interacting on a regular basis on the internet but have no technical knowledge and awareness of cybersecurity threats. [45] [13] [43].

A research by Ahmed et al. revealed that only 25% of Bangladeshi youths are aware of phishing techniques, making them highly vulnerable to online threats [14]. Similarly, older people, especially in rural places, are often the victims of financial fraud, including the Bkash scams, because of their lack of knowledge about online security [14].

Recent studies have shown that people who are above the age of 55 are more vulnerable to cybersecurity attacks, and thus are ideal targets for scammers [9]. In Bangladesh, about 70% of rural elderly people have been victims of cybercrimes due to zero cybersecurity awareness [22]. “Cyber threats to this group are further magnified in urban areas by the proliferation of devices such as the RFID system compromising ‘Flipper Zero’, and Wi-Fi cloning in public locations.”

Despite the rising digital risks, Bangladesh lacks proper cybersecurity training programs tailored for these vulnerable populations. Existing training methods rely on traditional, text-heavy approaches that fail to engage users effectively. Furthermore, there is a widespread lack of awareness regarding cybersecurity laws and best practices, leaving a significant portion of the population unprepared to handle cyber threats [32].

Gamification, on the other hand, is an emerging instructional approach that in-

creases engagement by converting learning tasks into game-like challenges with immediate feedback and social interaction. In cybersecurity education, tabletop and card-based games such as "serious games" have been shown to complement lecture based training by letting learners practice both attacks and defences in safe, story-driven scenarios with controlled environment [19]. For example, Riskio is a STRIDE-guided tabletop game where players alternate between attacker and defender roles while a game master facilitates reflection; studies using a Technology Acceptance Model survey found the game easy to learn and perceived as useful-especially among employees-when identifying threats and selecting countermeasures [19]. As a result, our research addresses the gap by proposing the development of a RPG-based (Role-Playing Game) cybersecurity training system. This approach offers an interactive and engaging way for users to learn about key cybersecurity concepts such as phishing, password management, Public Wi-Fi Risks, Malware and Ransomware scam Awareness, and Social Engineering. By incorporating decision-making models and realistic scenarios, the game allows players to test their knowledge in a safe environment and learn from their mistakes. Besides, the system comprises ultimate assessment and individual feedback for long-term knowledge retention. While there have been cybersecurity education programs in Western countries. Like the USPHS DoHSE's Stop-Think-Connect campaign ("Stop-Think-Connect Night Cam"). Many such initiatives have also been carried out by other countries, but Bangladesh is almost devoid of such activity..

The RPG-based computer training system has been designed after an in-depth analysis of existing cybersecurity training paradigms, gamification practices and cognitive reinforcement design principles. The platform features different levels providing structured learning with points or leaderboard ranking as a reward to the users who complete the levels. The system has also been made easily usable, with accessibility for people at different levels of digital literacy. To check its efficacy, a large-scale pilot trial is done, involving people of various age groups, genders, and locations. Feedback was gathered via surveys, focus groups and one-on-one interviews for the purpose of making refinements to the system prior to the full scale implementation. This multi-faceted strategy works toward developing a cybersecurity training which meets the young people and old curriculum requirements of Bangladesh, for them to acquire necessary skills to survive the digital knowledge space.

Initial qualitative data showed there is genuine demographic divide in the receptivity to the gamified learning, as adolescents (10-16) were keen to try it but the older generation (45+) were much more rooted with traditional learning methods such as seminars and articles. As a follow-up to the research above, an analysis was carried out of a gamified model with adolescents to assess the effectiveness of gamification on the receptive side of the demographic. The findings showed that, while both gamified and traditional interventions had a significant impact on cybersecurity awareness, the gamified one had statistically better results than the traditional one. To further refine and validate this approach, a large-scale study encompassing diverse age groups, genders, and geographic locations was undertaken, utilising surveys, focus groups, and one-on-one interviews. This multifaceted methodology aims to develop a refined cybersecurity training program that effectively addresses the unique needs of Bangladesh's vulnerable populations.

## 1.1 Research Gap

### Gamification as a means of improving digital literacy among Bangladesh's youth and elderly

Even though the concept of gamification is pretty vast in the Western world through video games or interactive classroom sessions, in other contexts, especially third-world countries like Bangladesh do not have sufficient knowledge or understanding of the do's and don'ts online. The most significant reason behind this is that Bangladesh is a developing country and the people of rural areas still lack accessibility of digitized technology because of the financial crisis, geographical inadaptability, ignorance and many more which makes them vulnerable to many severe cyber threats that are unknown to them. In our research, we aim to educate the younger generation (10-16 age group) and the older generation (45+ age group) to fix the problems in cyberspace where people are most vulnerable online [2], [18], [37].

### Lack of comprehensive framework for cybersecurity awareness

Traditional cybersecurity awareness programs often lack a comprehensive framework that addresses both motivational factors and deployment methodology [28]. This can lead to programs that are less effective in engaging users and achieving long-term knowledge retention.

### Limited application of gamification in cybersecurity education

Despite its potential, the application of gamification in cybersecurity education remains limited [31]. Since the needs of people creating games and the needs of people learning about cyber threats are constantly expanding, more research and development of new gamified solutions are required.

### Teenagers' lack of awareness about cybersecurity

The young adults, especially teenagers, are the most at risk mainly because they are immune to cybersecurity risks [24]. Such a situation calls for introducing programs like gaming applications promoting enhanced cybersecurity training among young people.

### Inadequate methods for cybersecurity training

According to Adams and Makramalla, traditional cybersecurity training methods, including in-person instruction and online guidance frequently fail to provide leaders and staff with the information and abilities they need [6]. Gamified learning systems can provide a more engaging and dynamic learning environment, improving skill development and knowledge retention.

### Limited effectiveness and influence of youngsters' cybersecurity education

Although there are various research projects and applications available, the effectiveness as well as the ability of cybersecurity education for children is still quite constrained [27]. It is crucial to offer more interesting, more motivating solutions, like a game-based action, or a play-based learning approach, to support children's awareness of cybersecurity ideas.

### Effectiveness of Cybersecurity Education Programs

A good number of the current cybersecurity education games and applications are made in the context of the research study, and therefore, their availability may be limited after the evaluation phase [27]. This also emphasizes the fact that the development of solutions for children which is targeted to address the current vulnerabilities of children should be sustainable and capable of being updated and modified as appropriate in child development over time as well as concerning the change in technologies and vulnerabilities.

### Gaps and limitations in existing studies on gamification for training in cybersecurity

Literature review of previous studies on gamification for cybersecurity learners has revealed some challenges and concerns including limited sample sizes, lack of assessment on learning achievement, and ambiguous findings [27]. Thus, one can conclude that there is a methodological demand for more systematically rigorous and controlled studies with large population samples and clear methods of evaluation.

### Limited research concerning gamification for older individuals

Previous studies examining gamification have mainly targeted young adults, and other population groups, including older adults, have remained inadequately studied [25]. This points to a deficiency of research on how gamification affects older adults generally, as well as their health, interpersonal relationships, and most importantly, their capacity for independent living.

### Methodological flaws in previous studies on gamification for older individuals

In the case of older adults, the identified shortages are critical because most studies apply simple gamified solutions, demonstrate short intervention times, have small sample sizes, and provide limited information about participants' technological competence [25]. Future research should target these gaps in a bid to enhance the quality and reliability of the results obtained.

### The Significance of validated measurement instruments in the field of gamification research

Currently, there are no tested measures specifically crafted for determining the effect of gamification on the aged [25]. Additionally, the triangulation of the instruments used in the execution of the studies highlighted the importance of the comparison of the different findings, making use of the instruments which have been validated to ensure the enhancement of the coherence and homogeneity of the knowledge in this area.

## 1.2 Research Objectives

The significance of cybersecurity awareness has grown considerably as digital engagements become integral to everyday existence. In Bangladesh, individuals across various age groups, both younger and older, are particularly susceptible to cyber threats, primarily due to a deficiency in cybersecurity knowledge and a lack of awareness regarding safe online behaviors. Traditional approaches to cybersecurity education, which typically encompass lectures and fixed educational resources, often fail to captivate a broad spectrum of age demographics, resulting in limited information retention and insufficient practical competencies. Research suggests that, despite the existence of certain gamified cybersecurity initiatives, such as the Beware, Cyber Hero Program, and Balloon Shooter, these programs frequently lack contextual relevance for the Bangladeshi audience. They typically employ a universal approach that ignores specific vulnerabilities and does not address the distinct behavioral tendencies prevalent within the Bangladeshi population, particularly when examining the disparities among different age groups.
The objective of this research is to fill the existing gap with the development of an appropriate in-context and in-culture gamified platform for the learning of cybersecurity that is specially fit for the child users between the ages of 10 and 16 and adult users between the ages of 45 and onwards in the region of Bangladesh. Primary tests shall define major elements of cybersecurity, designing an interactive learning platform addressing common cyber threats unique to the people of Bangladesh. Through the inclusion of elements like scenario learning, point mechanisms, and leader boards, among others, the solution proposed aims at enabling increased user participation, allowing knowledge to be transferred directly and practiced in practical terms, and inspiring better Internet habits that provoke better security. The pre-and post-intervention tests to be done shall allow the investigation of knowledge retention and improvement in behavior in detail, such that the platform is effectively and sustainably used in enhancing the awareness of the relevance of the importance of cybersecurity in the context of Bangladesh.

**RO1.** To carry out an initial process of evaluation to identify the ground level of knowledge of cybersecurity and the necessary elements for the successful gamified system among young (age 10-16) and old (age 45+) age groups in Bangladesh.

**RO2.** To design and execute a gamified cybersecurity awareness initiative, drawing on established approaches from existing games (such as Beware, Cyber Hero Program, Balloon Shooter, etc.) to enhance understanding, mo-

tivation, and secure online practices among young and older individuals in Bangladesh.

**RO3.** Developing features for a gamified cybersecurity training system, including interactive elements like rewards(stars) based on insights from the preliminary evaluation process..

**RO4.** To develop scenario-based simulation software to assess the practical application of knowledge in cybersecurity so that the audience can rehearse the appropriate online behaviour in situationally realistic scenarios.

**RO5.** Performing a post-intervention evaluation to analyze the influence of the gamified system on enhancing cybersecurity knowledge and fostering behavioural modifications among young and older individuals.

Unlike existing similar solutions, the new solution is aimed at being much more focused and enabling Bangladesh-specific cybersecurity awareness based on the user's age group. Unlike the majority of traditional cybersecurity learning platforms with poor engagement and outdated context relevance, it adopts a gamified approach to achieve high interactions and nurture a competition-driven mode for students. It makes the learning very real by adding location-based scenarios and adaptive learning to make for an incredibly topical, hands-on way of discovering cybersecurity. Expected contributions of the proposed solution not only include greater awareness of cybersecurity and more secure behavior among Bangladeshi users, but also a replicable model for culture-compatible cybersecurity education. This platform has the potential to be a key in influencing future global cybersecurity education and awareness initiatives, particularly for communities with varying educational needs. In the mixed context-response model and applied context-based learning, this work aims to push the cybersecurity education platform a step forward and make a great contribution to the development of an educated and robust online society.

## 1.3 Contribution

**The significant contributions of this research include:**

- **Methodological Rigour:** The study builds on the limitations of prior gamification research by involving the full player set, semi-structured interviews, statistical validation (t-tests, chi-square tests, confidence intervals), and systematic achievement analysis of learning.
- **Focus on Vulnerable Demographics:** The research targets and accounts for the following two vulnerability groups based on the results of the semi-structured interviews: adolescents (10-16) and the aged (45+). The targeting of two groups is novel in the research and follows the expected patterns of learning and vulnerability.
- **Localised and Contextualised Design:** The gamified platform CyberGuardChronicles uses nation-specific scenarios such as email phishing, Bkash

fraud, Wi-Fi security, and password security vulnerabilities. The localization makes it more regional and practical for real-world scenarios and addresses the limitation of global standardized solutions.

- **Controlled Study Comparison:** Unlike current works that typically involve only pilot testing of gamified technologies, this research employs a controlled study format comparing traditional methods with gamified RPG-based approaches, providing empirical evidence on effectiveness and engagement.

## 1.4 Thesis Structure

For the purpose of this thesis, which consists of nine chapters, the following structure has been defined:

**Chapter 1: Introduction**

In this chapter, the research context was introduced, and the significance of cybersecurity awareness is highlighted along with the major objectives of the study. It also identifies and fills the research gap and provides a snapshot of the particular focus on gamified cybersecurity education for different age levels in Bangladesh.

**Chapter 2: Related Work**

The second chapter is based on a review of previous research and studies on gamification in cybersecurity and similar educational strategies. To determine the approach of the gamified system for this study, the background and relevant literature are evaluated.

**Chapter 3: Methodology**

In this chapter, the research methodology is described through the stages of designing, developing, and testing the gamified cybersecurity training platform. Additionally, this chapter discusses the gamification strategies adopted and the participant evaluation process.

**Chapter 4: Semi-structured Interview**

This chapter presents both the process and analysis of semi-structured interviews conducted with children (10–16) and adults (45+) to identify their cybersecurity awareness levels, behaviors, and learning preferences. Insights from these interviews directly informed the design and development of the gamified learning system.

**Chapter 5: Game Design and Development: CyberGuard Chronicles**

This chapter details the design and development of CyberGuard Chronicles, an RPG-based educational game that teaches cybersecurity through five progressive levels addressing phishing, password security, public Wi-Fi risks, malware, and social engineering scams. The game also includes local cases of Bangladesh and characters,

pilot testing that helps streamline gameplay mechanics and sound to maximize the participation and education of the users.

**Chapter 6: Evaluation: Comparative Controlled Study**

The research provides a statistical analysis of the learning results based on the controlled comparative study between game-oriented and conventional cybersecurity education. The findings reflect that the methodology of the role-playing game provided significantly better improvement (4.61 points) compared to the traditional methods (2.82 points), with such an advantage being statistically significant and regularly observed at the national and regional levels. The researchers used the t-tests and ANOVA to substantiate such findings and proved the efficacy of the game-based approach irrespective of the indicators of demographics. Overall, the results significantly support the superior efficacy of gamified learning in cybersecurity Education.

**Chapter 7: Discussion and Future Possibilities**
This section elaborates on the findings of the data analysis on age  location-based awareness in the field of cybersecurity. Game-based learning revealed significant improvement (4.6 points) compared to conventional (2.8 points) in the pre-  post-intervention assessment environment. The findings in geographical settings reflect the strength and efficacy of cybersecurity education.

**Chapter 8: Conclusion**

The chapter summarizes the results and findings of the research with a focus on the effectiveness of the gamified solution and the potential future research avenues.

# Chapter 2

# Related Work

## 2.1 Background

This chapter indicates how cybersecurity awareness is relevant in the current-day digital environment, especially among youngsters and the elderly, who are the most vulnerable and who, in most cases, do not possess the required knowledge to be safe on the internet [22]. It presents how cybersecurity education and digital literacy in Bangladesh are still not very high, as is the case in western countries. The section about demographics and age groups specifies that although adolescents are habitually regular users of the internet, they are likely to underestimate the dangers of online activity and engage in irresponsible behavior, yet aged people are unable to keep up with the ever-evolving technologies, which makes them even more susceptible to being deceived by spam/phishing and fraud [14],[25]. The chapter demonstrates gamification as an emerging pedagogy of learning with the intention of overcoming these challenges by using approaches of game structure to make cybersecurity learning more attractive and effective. Gamification enhances motivation and triggers learners of different age groups to understand better online protection strategies through its system of challenge, reward, and narrative, as illustrated through research of its effectiveness in academic and training institutes [1],[4].

### 2.1.1 Cybersecurity Awareness

In the modern world of rapid digitization, consciousness about cybersecurity is essential and especially among such vulnerable populations as youngsters and the elderly [22]. Although children in Western nations are instilled with the importance of parental control and other basics of cybersecurity, these measures are not commonly applicable in Bangladesh. Cyber security may be considered as policies and controls that are implemented to protect the computer systems or networks against random and unauthorised access, illegal disclosure of information, or deliberate change or destruction of information. It includes a variety of security measures, including administrative controls (like security policies and user training), technical protections (like firewalls and antivirus software), and physical security measures (like access control systems). Educating people about potential cyber threats, vulnerabilities, and safe online practices is a crucial component of cybersecurity awareness. This entails being aware of the dangers of engaging in online activities, identifying typical cyber threats (such as malware, phishing, identity theft, data breaches, and social

security number breaches), and putting preventative measures in place to safeguard digital assets and personal data.

### 2.1.2 Gamification

As basic Cybersecurity training was proving to be difficult to grasp for the people of the targeted age groups, people started losing their interest in it. To make people fascinated towards it by giving a more engaging experience, the concept of "Gamification" was implemented in it. Gamification is the execution of elements and concepts of game design outside of the gaming environment [4]. This approach will utilize the game's ability to fascinate and motivate in order to enhance the learning and problem-solving abilities of the end user. It can change serious, text-based training approaches, practiced in learning about cybersecurity into a set of exciting games. The use of gamification may enhance the learning, motivation and relevance of teaching and learning cybersecurity by incorporating game features such as; challenges, restitution, status reports, and narratives. This is illustrated by a research project known as eSG2 which attempts to provide students with creativity and entrepreneurial thinking through gamification [1]. The course is made up of normal class lectures, guest speakers from the business world, serious games, homework assignments, as well as team-based play-offs [4].It also shows how gamification may be adapted for use in various learning environments and learning environments in third-world developing countries.

Enumerated in this paper are the compelling reasons to call for an effective cybersecurity education that addresses the needs and challenges faced by all age groups of learners chiefly in developing countries like Bangladesh. Thus, gamification offers a feasible solution for increasing cyber threats' security awareness and the appropriate online behavior of the mentioned susceptible populations.

## 2.2 Literature Review

Cybersecurity awareness becomes critical as online threats continue to grow, particularly among young people who spend large amounts of their lives online but are rarely equipped to remain vigilant. With studies proving low awareness of cybersecurity, users, primarily teens, are at risk of falling victim to phishing, identity theft, and online fraud. According to Nabi, cybersecurity awareness in Bangladesh is below par, and it was also highlighted by Siddiqui that awareness programs are urgently required in order to keep pace with growing threats [10][48]. Likewise, a study by Rahman also noted that teens are still one of the highest groups targeted due to their weak knowledge of online security. High-tech digitalisation has also seen a steady number of malware, cookie tracking, and data intrusion incidents, which highlights the importance of formal awareness programs and tougher protection measures [33][30]. Traditional pedagogical methods, such as lectures and texts,

normally neither engage nor retain students for a long time. As identified by Alotaibi and Alzahrani, traditional methodologies are less effective than interactive methodologies in retaining user motivation and knowledge over a longer timeframe. One of the solutions provided by gamification is to incorporate points, rewards, and leaderboards, for instance, to make cybersecurity courses more enjoyable. As indicated by Saleem et al., Sağlam et al., and Tempestini et al., studies, gamified learning enhances participation, motivation, and knowledge retention across a variety of ages [21][41][52]. Yet their success hinges on properly designed evaluation and data-based verification. Reese et al. and Tally et al. emphasise that if cybersecurity interventions are not properly evaluated, they may be ineffective or even deceptive [17][43]. Despite remaining challenges like scalability and long-term adherence, gamification offers a potential method of bringing cybersecurity education more practically and effectively, not least in developing nations like Bangladesh [7][26].

### 2.2.1 Cyber-threats in Bangladesh

With the rapid digital transformation of Bangladesh cyber threats have increased rapidly, which increases the relevance of Online Scams, Phishing, Identity Theft, Cookie Tracking, Virus or Malware. In Bangladesh, cyber fraud incidents increased by 34% from 2017 to 2019, targeting mobile financial services (MFS) like bKash, Nagad, and Rocket, and affecting 3,500 fraud cases and losses about BDT 50 million in 2022 [35]. One of which, phishing, continues to be a popular attack method, as 40% of the total cybercrimes reported in 2019 were phishing and identity theft (BCT 2022). According to a survey, 67% of Bangladeshi internet users received phishing emails and 12% fell prey to phishing in 2020 [34]. Digital platforms are increasingly used, and their use has also raised privacy concerns, as 82% of Bangladeshi websites do not implement proper cookie consent, which results in unauthorised data tracking and identity theft [35]. In a 2019 Facebook data breach over 3 million Bangladeshi accounts were compromised [30]. Cyberattacks are still booming, including malware and ransomware, involving 63.2% of all cyber incidents in 2020 being malware-related, and more than half are Trojans or ransomware [34]. Significantly, the incident of Bangladesh Bank Heist in which hackers exploited malware to trick the SWIFT banking system to steal $81 million goes on to be a stunning acknowledgement of the country's vulnerability [35]. However, institutional weaknesses further compound these threats, given that many government agencies do not have applicable cybersecurity frameworks and in fact few government district websites were hacked in just 24 hours in 2018 [30]. Selection of these cyber threats is justified given that they tend to cause major risks to financial and personal privacy, occur at a high rate and affect individuals, businesses and government institutions, and hence there is a dire need for cybersecurity reforms and awareness campaigns for Bangladesh digital future.

### 2.2.2 The Importance of Cybersecurity Awareness

In the modern world, where cyber threats are increasing and young people are particularly prone to falling for them, it is essential [29]. For people to avoid falling

prey to cyber criminals, then they need to have some form of knowledge about their actions online and the impacts that these behaviours will have on other users. A study conducted by Nabi identifies that cybersecurity awareness in Bangladesh is not satisfactory, and citizens become an easier target for an attack via web [10]. Likewise, Siddiqui talks about current cyber threats in Bangladesh and identifies a necessity for a rise in cybersecurity awareness programs in an attempt to counteract [48]. All such observations confirm a necessity for individual awareness programs for groups, specifically for youth, who become an easier target for a cyber attack. The youth, especially the teenagers are the most reliant targets for cyber criminals owing to their ignorance and poor knowledge of cybersecurity [24]. Because they have access to a wide variety of digital devices and virtually every opportunity the Internet presents, teenagers are particularly susceptible to engaging in harmful online activities. This makes it important to develop cybersecurity education and sensitization programs that can engage the teenager and teach him/her how to handle the digital world.

### 2.2.3 Ineffective Traditional Approaches

Previous cybersecurity awareness training is known to have poor structures in so far as motivational perspectives are concerned and the nature of deployment [28]. In turn, this can result in developing programs that are not as effective in user engagement and knowledge retention over longer periods. Lecturing and online quick tips are not the best ways to transfer the adoption knowledge and skills to the employees and other leaders in the organization [6]. On the same note, the research conducted by Alotaibi & Alzahrani in IEEE Access noted that gamified learning strategies have the potential of being superior over traditional methods in that they allow active learning and motivation in the learner, unlike the use of lectures and other print media that do not, for example, appeal to adolescents [33].

### 2.2.4 Gamification: An Engaging Alternative

Particularly in cybersecurity, gamification can be used to offer more enjoyable methods of imparting information to teenagers and motivate them to make good use of cybersecurity. To lend credibility to this argument, Pramod discusses the viability of the conventional methods of cybersecurity learning and how gamification can cover the inertia that exists in engagement and retention of information [50]. The elements may be scores, rewards, and rank boards, strenuous tasks, i.e., to better the performance of teaching and imparting information about cybersecurity as an entertaining way to grasp [31]. Fortunately, the integration of gamification has been largely accepted as a potential learning activity to promote better learning conditions [21]. Recent reports have stressed on cybersecurity awareness training programs that should be age-specific. For instance, Sağlam et al. conducted a systematic literature review on cybersecurity education for children, highlighting the effectiveness of gamification-based learning techniques in enhancing children's understanding of cyber threats [41]. Similarly, Mclaughlin explored learner choice in

cybersecurity training and whether individuals prefer gamified approaches, indicating that motivation varies across different demographics [39]. Studies have further reinforced the importance of gamification in cybersecurity education. Tempestini et al. explored game-based informal learning strategies for young adults and found that engagement increased significantly with interactive approaches [52]. It encourages and prompts learners' participation in a gamification system. The elements of gamification that are utilized often in e-learning, and those that have a significant impact on students, include points, leaderboards, badges, and levels, according to Saleem and his team.

### Related Works on Gamification and Cybersecurity Awareness

The use of gamification to raise cybersecurity awareness has also been studied by several researchers. and several gamification platforms had been developed to raise awareness against cyber threats and engaging hands-on training of cybersecurity. Here are some of the related works-

- **Cybersecurity Awareness Framework**
  This program introduced a gamification technology named "Cyber Hero Program" and it was planned to create awareness for cyberspace. The Cyber Hero Program Held three components as a gamification technology, and it was labeled as "Pre Test", Gamified Training and finally "Post Test". All these combine the framework of the Cyber Security Awareness Framework, known as the Cyber-Hero program. Moreover, in the "Gamified Training" phase, students find out how to develop secure passwords for their social media and more [28].

- **Gamification Awareness Prototype**
  This paper proposes an intelligent gamification method for children to enhance their awareness of cybersecurity, especially on Facebook Messenger. The interface is friendly, from where students can gasp the tool and can avoid falling prey to danger [31].

- **Cybersecurity Game**
  A game named "BEWARE" was developed to raise awareness about cyber threats and cybersecurity, and it helped by simulating real-life situations for teenagers to train and make decisions that could educate and prevent cyber threats. The game "BEWARE" helps raise cybersecurity awareness in teenagers by simulating real-life scenarios and training users to make decisions that prevent cyber threats [24].

- **Attacker-Centric Gamification**
  In the approach of using gamification technology for training and training the mind from the attacker's perspective. This approach is really powerful because the trainee can understand the attacker's motive before getting compromised [6].

- **Multiplayer Cybersecurity Game**
  The work described in this paper is a conceptualisation and assessment of an educational computer game named 'Security Empire.' The game requires players to design an efficient green energy organisation whilst following good information assurance procedures [5].

- **Game-Based Learning and Hands-On Labs**
  Consequently, this paper offers a summary of the discovery method that uses games and interactive labs for the teaching of cybersecurity to high school students. The authors also established that undertaking such an approach helped them educate the students on cybersecurity issues and encouraged them to further their studies on the subject [8].

- **Gamified E-learning**
  A survey of the research on gamification in online learning environments is presented in this work. The authors also concluded their work and came. up with the knowledge that gamification can be executed to improve overall motivation and cater to learning achievements among students [21].

- **Gameful Interventions for Older Adults**
  This paper reflects a systematic literature review focused on the use of gamification for older adults. The authors established that through the use of gamification, cognitive and physical health, as well as mental health would be enhanced among the elderly [25].

- **Generalized Cybersecurity Game for Children**
  In a study on the effectiveness of gamification technology within Bangladesh demographic context, a basic game named "Balloon Shooter" was developed. The main objective of this game was to enhance and develop general cybersecurity knowledge among younger audiences mostly covering children [12].

- **SherLOCKED**
  A Detective-Themed Serious Game: Jaffray et al. designed SherLOCKED, a cybersecurity education game that engages players in solving security-related mysteries [23].

- **Teaching Cybersecurity Awareness Through Gamification**
  Potato Pirates introduced a gamified cybersecurity education platform aimed at helping educators teach fundamental security concepts in an engaging way [40].

- **Secure Arcade – A Gamified Defence Against Cyber Attacks**
  Loesch et al. introduced Secure Arcade, a gamified platform designed to train individuals in defensive cybersecurity strategies [36]. The study demonstrated how hands-on learning through gamified challenges could improve security awareness and decision-making skills.

- **Zero-Day Cybersecurity Awareness Game**
  Abu-Amara et al. introduced the Zero-Day Awareness Program (ZDAP), combining pre- post-game phishing attack simulations, surveys, and a five-level interactive game. It covers critical concepts like weak passwords, social engineering scams, cracked software, and phishing with an embedded chatbot. Tested on 23 employees, results showed an average awareness improvement of 84.7% and a 77% reduction in phishing susceptibility [44].

- **Riskio, A Card-based TableTop game**
  Hart et al. developed Riskio, a serious game designed to improve cybersecurity awareness and education through risk assessment simulations. The game allows players to alternate between the roles of attacker and defender, enabling them to understand both perspectives and assess the consequences of cybersecurity decisions in realistic scenarios. Results showed that players gained a deeper understanding of security risk management and human factors influencing decision-making [19].

Such studies illustrate the possibilities of applying gamification of cybersecurity practices irrespective of age and learning environment. Despite its potential, gamification techniques are not widely used in cybersecurity education [31]. More effort should be paid to create new forms of games and other effective applications of gamification in the frameworks of the cybersecurity concept, and young people in particular.

### 2.2.5 Effectiveness Through Evaluation

Without the help of adequate data or study, there is no effective way to develop and assess cybersecurity solutions. Methods such as gamified learning systems, studies of multi-factor authentication systems, or phishing awareness programs can only be valid if they are backed up by comprehensive studies and valid research. A poorly designed evaluation method will make any solution unadoptable and can make it ineffective as a whole, and in the worst case, can make the whole study counterproductive. Earlier research indicates such a danger: [43] and [17] have reported that employees that primarily received phishing awareness through scattered and informal sources were susceptible, even an usability research on two-factor authentication practice pointed the analysis at adoption issues through ignoring the fact that real users work in a way that does not align with their design [43] [17]. Similarly, the secure key management of email research and a tutoring trigger-action programming system(Kuang et al.) research presented fine-tune usability concerns that cannot be identified without conducting rigorous studies [47]. These research examples demonstrate that to capture pertinent behavioural patterns and cognitive factors affecting performance, it is critical to do an evaluation rather than solely rely on task completion rates. The various methodological strategies provide some complementary advantages when it comes to untangling these factors of evaluation and adopting mainstream solutions. The potential of immersive techniques to manifest genuine decision making processes under high pressure settings, represented when a set of scenarios involving newsworthy or provocative events are played with

various participants acting in different roles, is demonstrated by scenario-based role plays such as the study of Zamfirescu-Pereira et al., who work with journalists using AI-based checking tools and is quantifiable in terms of privacy and literacy improvement in the sample of middle school students conducting a design based research. The systematic literature review is valuable, according to Wolfswinkel et al., which visualised the gap of examination routines and identified a common usage of small samples and self-reported measures [53]. Moreover, recent research has shown that mixed-method evaluations, augmented reality-based phishing training, have shown an accuracy of 93%. These new interventions and implementations adhered to eye-tracking and post training evaluation to 93 smile design increased its default system as the development of its cybersecurity self-efficacy related dwellings, and CALYPSO platform bored its cybersecurity self-efficacy-related dwellings with iterative design adopted together with these studies reinforce the idea that cementing cybersecurity interventions through rigorous and varied evaluations designs both ensure usability and effectiveness, hence helping bolster user awareness and influencing wiser and safer online navigation [46], [55].

### 2.2.6 Established Study Design Approaches

The study of cybersecurity awareness and implementation of gamification utilises a heterogeneous collection of methodological frameworks. These often include controlled laboratory environments to conduct tests, field tests and qualitative interviews, role-play tests, and extensive literature reviews. In this section, the studies analysed are separated and divided based on how they were designed and compared to determine how each was evaluated, resulting in finding their strengths and figuring out limitations.

#### Survey and Field Studies

Field- and survey-research methodologies are empirically sound, and hold ecological validity through the experience of authentic practice and assessment of attitudes. To ensure data integrity, McCall et al. implemented attraction checks and practice procedures in order to secure high-quality data within a controlled survey of TriggerAction Programming (TAP) tools with 447 participants [38]. An experiment design was developed which allowed for a quantitative comparison of the differences between system-specified anti-patterns and user perceptions of undesirable patterns of behavior. Likewise, Reese et al. developed an experimental field case, conducted over two weeks and the participation of 72 individuals, focusing on two factor authentication (2FA), which documented authentication behaviour and followed it with post study interviews [17]. Taken together, these studies demonstrate the potential utility of large-scale longitudinal surveys in elucidating understandings of usability, if perhaps at the cost of depth for breadth.

#### Laboratory and Experimental Studies

Usability laboratory designs are often used to control independent variables to determine usability results. The within-subjects laboratory study by Ruoti et al. involved 47 dyads, which were asked to compare three e-mail key-management systems, all of

which are considered secure. Researchers assessed the systems on three factors: Success in completing the task, time taken, and the extent of system usability. Schoni et al. carried out a between-subjects study with 117 subjects to assess augmented reality-based phishing training interventions (interactive, text-based, and particularly), respectively. The study employed a comparative approach, evaluating both behavioural variables, consisting of eye tracking of connection data and classification degree, while standardised questionnaires such as NAS (North American Space Flight Evaluation) of Crews, SUS, UES (User Experience Survey) of SF, and HAIS (Health, safety, and comfort in space) Questionnaire were used [55]. Miner et al. conducted a mixed-method study devoted to virtual reality and a sample of 21 participants. During the experiment, their biometric respiratory data were measured at the same time as immersion and usability values were being collected [49]. Despite the robust external validity afforded to these studies, as well as the fact that they made direct comparisons of outcomes possible, they have common limitations, such as relatively small sample sizes and the use of artificial laboratory contexts.

### Design-Based and Game-Based Approaches

The evidence suggests that modern scholarship often contains recursive development and testing loops, with more focus on the development of the applied intervention than on complying with traditional paradigms for hypothesis-testing. Using a design-based research (DBR) model, Khan et al. (2024) provided students with a program on privacy education in the context of the schools, conducting curriculum refinement through the use of classroom observation, pre-/post assessment, and semi-structured interviews [45]. The C.A.L.Y.P.S.O. was a gamified system that enabled the selected variables of self-efficacy to be persistently manipulated, which was later validated through play-testing with both experts and beginners in the field of cybersecurity, as reported by Krsek et al. (2024) [46]. A similar strategy was evidenced by Miner et al. (2024) employing the virtual-reality experience that they called Stairway to Heaven, combining usability measurement and learning by doing [49]. Collectively, these approaches illustrate the benefits of iteratively collecting information with a learned bias towards ecological validity at the cost of tight experimental control.

### Qualitative and Role-Play Studies

Descriptive research designs are used to provide information in more depth about the activities that users perform, as well as their perceptions and decision-making processes. The importance of the contextualised tips and training in the development of safe behaviours was proven through research work carried out by Kumar et al, which used email communications and workshops as an analytical mode to focus on anti-competency awareness among middle-aged office workers [43]. Grounded theory interviews, carried out with twenty-four administrative workers by Tally and others, indicate that informal learning as it relates to IT training is more dominant than formal IT training. Sohrawardi et al. exposed 24 journalists working in simulated newsroom environments to scenario-based role play, complemented with traditional verification efforts but also with an alternative application of AI-based deepfake detection software [51]. These paradigmatic strategies emphasise the deviance regarding the upper capability for generating deep, text-based interpreta-

tions; nevertheless, the outputs would not be generalisable in the same manner as experimental approaches.

**Systematic Reviews and Knowledge Synthesis**

Systematic reviews are syntheses of much of the knowledge base compiled from the results of many studies. Huang et al. did a systematic review which included 3926 papers focused on cybersecurity and privacy games, and they used five-stage models to guide their methodology and analysed 93 papers out of 3926 papers identified by codings according to design goals, target groups, and evaluation methods [54]. In general, the paper found that most internet-based games do include pre- and post-knowledge assessments and surveys, while none use behaviour logging and standardised usability scales to evaluate systems. Although these reviews are lacking in primary empirical validation, they nonetheless outline methodological trends and gaps in the research that ultimately can guide the design of future studies.
**Comparative Insights**
Methodological stringency varies in diverse designs:

- **Surveys and field studies** show significant scalability, though they could potentially oversimplify complex behavior.
- **Laboratory experiments** guarantee control and comparability but lack realism.
- **Design- and game-based paradigms** privilege the processes of iteration which produce concrete interventions, while sacrificing some experimental precision.
- **Qualitative and role-play methods** offer contextualized insight into user strategies but may be less generalizable.
- **Systematic reviews** involve exhaustive coverage and synthesis, but they rely on secondary data.

Collectively, how well the interventions are tested by Controlled studies. Then, the hidden factors that influence users are shown by Qualitative work. Lastly, the findings within larger trends are placed by reviews. Altogether, these approaches provide support for the evidence.

### 2.2.7 Challenges and Opportunities

Accounts of dozens of cybersecurity education games and applications developed in research efforts rarely achieve a stage beyond experimentation or pilot testing that brings them to a point of broader adoption, limiting their overall outcomes for applications in practical contexts in spite of promising empirical performance.
Roepke et al. stress the need for highly elaborated gameplay and all its elements, like adaptive feedback, increasing difficulty, or even storytelling, in order to make players absorb the fundamentals of anti-phishing behavior and even get more engaged [20]. More recent interventions, like the Zero-Day Awareness Program (ZDAP), observed

an 84.7 per cent awareness increase and 77% phishing susceptibility reduction and thus show the great potential of gamification in educating towards cybersecurity [44]. Still, several studies remain constrained in small scales or pilot test groups and thus minimise the level of generalizability. Sustenance and flexibility remain valuable concerns. The cybersecurity training programmes should also continue to acquire and refresh skills in due course, as argued by Onduto, because cyber threats are fluid [26]. Most gamified solutions, however, lack a mechanism for frequent refreshment, thus rendering them less effective in the long term. Methodology is another weakness in studies, in that many of the works use small-scale mindscapes, concentrate on negative feedback, but never closely study the learning outcomes, or make the conclusions vague [3]. This variability is also reflected in the State of Knowledge review of games for cybersecurity, in that whilst questionnaires and pre-/post testing are common, not many studies adopt the longitudinal approach or seek to involve diverse populations, which is fundamental to long-term behaviour change. However, there still exist large-scale possibilities of innovation. As shown by Zahir et al., the combination of physical and digital gamification features, i.e., board games with online simulation of activities, could help people to improve their learning processes [7]. The recent trends further reflect this possibility: the post-training detection rate of augmented-reality training went to 93; phishing training mitigating cognitive biases, including urgency and fear, achieved much higher hit rates, and the design-based research cycle-grounded classroom intervention soon significantly broader parameters of privacy and security literacy [55][45]. As more people have access to mobile tools, faster internet access, and novel technologies like VR/AR and AI-powered chatbots, game-based education in the context of cybersecurity, albeit untapped, is likely to provide scalable, versatile, and interactive training solutions with a range of applications across various audiences [1].

## 2.3 Our Research

While existing literature addresses using gamification in cybersecurity training, our contribution is in its sole, focused investigation of the Bangladeshi populace, youth (10-16 years) and older adults (45+ years) in urban and rural areas. Unlike in previous works, such as a single age group or a general model for gamification, in our work, contextual and cultural factors are included in game design. Besides, our iterative development model, through theme analysis of participant interviews, is guaranteed to have a game that covers the most important gaps in cybersecurity awareness in the target community. With its careful, data-driven model, a more relevant and effective educational tool can be constructed.

Whereas many studies exist regarding gamification as a cybersecurity awareness method, a number of research gaps still exist. Other available solutions, like Cyber Hero Program [26], BEWARE [22], Riskio (Hart et al.,), or Zero-Day Awareness Program (Abu-Amara et al.,), were generally aimed at professionals or single age cohorts [19][44]. These researchers tended to focus on interactivity or short-term behavioural change as opposed to long-term behavioural change. Moreover, there were not many works which referred to socio-cultural circumstances and geographically focused cyber threats, especially in developing nations, such as Bangladesh. The other shortcoming is the limited scope of evaluation. Although games such as Bal-

loon Shooter [12] were aimed at local awareness, they were not tested for usability or compared with each other in terms of demographics [12]. Old training approaches are also prevalent, although they are not very effective in engagement and retention of knowledge [6][26]. This paper will fill these gaps with a context-aware, gamified cybersecurity awareness system targeting the Bangladeshi youth (10-16 years) and adults (45 years and above). It combines semi-structured interviews to establish behavioural requirements and forms a localised gamified prototype based on the actual dangers like phishing, mobile fraud, and identity theft. However, it is important to note that, unlike earlier articles, this study aims at learning across generations, the relevance of a culture and repeated assessment, to offer a scalable and inclusive model to enhance cybersecurity awareness among Bangladeshis.

# Chapter 3

# Methodology

In this chapter, the research design and methodological outline used in this study are mentioned. It describes the logical sequence of achieving research goals, dwells upon the systematic application of a gamification strategy to promote cybersecurity education. The chapter describes every step of the research, starting with the selection of the participants, the collection of the data, and its analysis, up to the design, development and testing of the gamified training module. It further describes how these steps shown in Figure 3.1 were incorporated to make the results reliable and valid.

## 3.1 Methodology

The research design of this specific research project allocates a very pivotal position to the systematic and intentional application of gamification strategies with the final objective of improving education in cybersecurity. The entire process has been carefully segmented into various phases, some of which are participant selection, data collection, data analysis, game development, and testing. All these steps are discussed in detail in the subsequent sections. The following flowchart (see Figure 3.1) illustrates the step-by-step methodology used in this study, providing a visual overview of the research process-

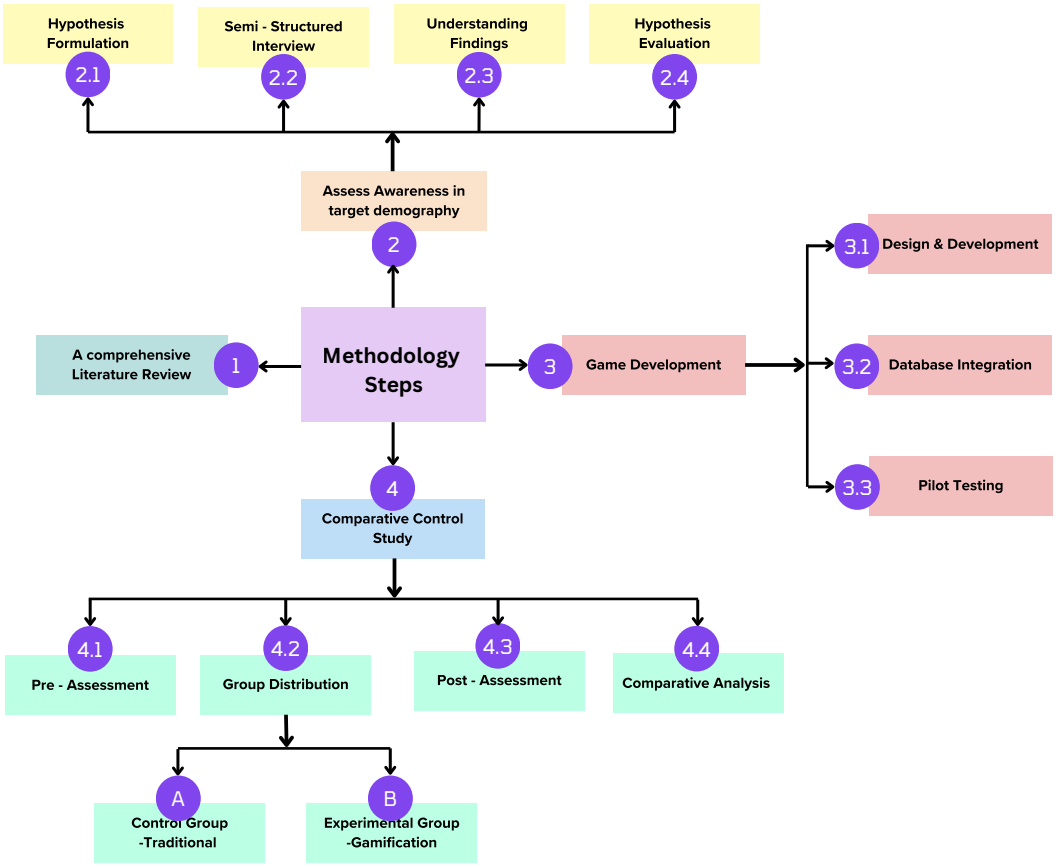



Figure 3.1: Methodology Flowchart

## 3.2 Understanding Gamification Strategies in Cybersecurity Awareness

A comprehensive literature review on understanding gamification strategies in cybersecurity awareness was conducted in an attempt to seek and evaluate existing studies, frameworks, and methodologies for gamified cybersecurity training. The review was for the purpose of identifying prevalent approaches, strengths, and weaknesses, and with those found, a new, original gamified approach specifically for the Bangladeshi community could then be developed. In an attempt to search and choose relevant studies, academic databases including IEEE Xplore, ACM Digital Library, Springer, and Google Scholar were involved with the keywords "gamification in cybersecurity," "cybersecurity education," "game-based learning," and "gamification frameworks". The selection included studies specifically dealing with gamification for cybersecurity awareness for adolescents and adults first and foremost. Qualitative and quantitative studies are both included in an endeavour to have a balanced view of the matter in question. Studies about traditional learning methods, such as lectures and reading, are included in an endeavour to present gaps effectively addressed with gamification. Additional care in choosing studies with high emphasis is placed in immersive and interactive settings, specifically for adolescents and ageing adults who react positively towards such settings.The literature

analysis revealed several noteworthy initiatives in gamified cybersecurity education. For instance, the "Cyber Hero Program" involved a systemic model with pre-tests, gamified training, and post-tests to educate users about secure password creation and web security. Similarly, the "BEWARE" game represented real-life scenarios to educate adolescents about identifying and counteracting cyber-attacks. Other studies addressed newer methodologies such as attack-focused gamification, multi-user cybersecurity games, and hands-on labs and training through games mixed and matched together. Bearing these in mind, most of the studies did not take into consideration the cultural and contextual-sensitivities especially in underrepresented countries such as Bangladesh. Based on them, these observations led to the necessity of tailor-made alternatives to complement the unique needs and interests of youngsters and older adults in Bangladesh.

## 3.3 Evaluating Cybersecurity Awareness Among People in Bangladesh

This section provides a brief introduction to the pilot screening of awareness conducted before developing the gamified solution. The study observed the understanding and response of people across different age groups and regions of Bangladesh regarding common cybersecurity threats and thus provided an empirical basis for the design of the ensuing system.

### 3.3.1 Hypothesis Formulation

Three hypotheses were formulated to examine the relationships between age, geographical area, and preventive behavior:

**Hypothesis 1: Both age groups would be equally interested in gamified learning.**

**Hypothesis 2: Urban respondents would be more knowledgeable about cybersecurity than rural respondents.**

**Hypothesis 3: Urban adolescents would exhibit stronger preventive behaviors.**

These hypotheses guided the planning of the interviews and the following statistical tests.

### 3.3.2 Semi-structured Interview

Semi-structured interviews were conducted with respondents in both rural and urban areas, who covered adolescents (10–16 years) and aged people (45 + years), in an effort to assess awareness levels, behavioral patterns and misconceptions about phishing, weak passwords, Internet scams and Wi-Fi security. The snowball method was used to select the respondents among two research teams, in which the interviews in the rural area began with the major respondents in each age group who referred others to them, and all interviews were conducted in Bengali in an effort to

enhance understanding. Ethical clearance and consent came prior to respondents' participation. Semi-structured interviews were conducted in one-to-one mode with 70 participants in total. Among them, 42 participants in the age limit of 10 to 16 years and 28 participants aged over 45 years. The research consisted of 7 respondents aged between 65 and 72 years old which we did not include in the final analysis due to the lack of availability of online access. All the interviews in the duration of 20-25 minutes were done in the most favorable places.

### 3.3.3 Hypothesis Evaluation

Statistical analysis used independent t-tests, chi-square tests, and confidence-interval estimation to explore region- and age-based differences. Results confirmed the existence of a clear urban–rural divide and strong age-related inequalities in digital safety measures, thus confirming the importance of having an awareness tool designed for unique settings.

### 3.3.4 Understanding the Findings

The research showed that young urban users had higher technical awareness, whereas aged and rural users did not receive exposure to safe online behavior. These observations directly influenced the development of specific in-game lessons and challenges which deal with phishing, Bkash frauds, password hygiene, and Wi-Fi security in CyberGuard Chronicles.

## 3.4 Gamified Solution Design and Development (CyberGuard Chronicles)

It is designed with Unity with the support of Firebase. It enables a sequence of tutorials and Heads Up Display (HUD) features including mini-maps, waypoints, and doorways in addition to role playing interactions serving to maintain a sense of clarity, engagement and an enforcement of enriching sequence of the learning behaviours of progression. It was developed based on the findings of semi-structured interviews that pointed at significant cybersecurity threats to children aged 10 to 16. The information based on the analysis was used to set the features that were to be included in the game, including:

- **Scenario-Based Challenges:** Real-life scenarios, such as identifying phishing emails or setting strong passwords, were incorporated.
- **Levels and Progression:** There were 5 levels in the game that were centered on the a. certain concepts of cybersecurity.
- **Gamification Elements:** Stars as badges and Points were integrated to motivate and engage players.
- **Cultural Context:** Visuals, language, and scenarios were adapted to the Bangladeshi context to enhance relatability and effectiveness.

An iterative development process was followed, involving regular feedback from a focus group to ensure the game's content and mechanics aligned with the learning objectives.

## 3.5 Evaluation: Comparative Controlled Study

In order to enrich the primary study and increase the credibility of the results, we conducted a control study. This paper compared the performance of normal teaching techniques with the scheme of gamified learning that we adopted. We considered only children between the ages of 10-16 since by doing so, we will be able to observe the impacts of gamification on cyber safety awareness of children. Moreover, 92% of older demographics have disagreed on trying gamified technology to learn about basic security practices. As a result, this control study aimed to evaluate the knowledge and learning effectiveness of the students of target age group in five key cybersecurity areas most relevant to adolescent internet users in Bangladesh based on our initial research.

1. Phishing attacks
2. Weak password threat
3. Free/Open Wi-Fi vulnerabilities
4. Virus, Malware threats
5. Bkash fraud, Fake Charity, and other social engineering scams

In the following section, the design and steps of this control study will be explained.

### 3.5.1 Participant Selection

In this study, we enrolled 96 children aged between 10-16 years. The respondents were from both Urban and rural schools in Bangladesh. They are the most frequent Internet device users so they are a prime target to learn about cybersecurity. Multiple sampling strategies were employed to ensure diversity:

i. **Snowball Sampling:** Initially selected students referred their peers and classmates, creating a natural chain of recruitment.

ii. **Voluntary Response Sampling:** Students who were enthusiastic about digital learning volunteered to participate after being informed of the project's purpose.

iii. **Convenience Sampling:** Some of the students were chosen due to convenience of access and during the school sessions.

This sampling strategy had the advantage of enabling the researchers to recruit a diverse population besides balancing the research limitations of time, availability, and access. Approaches to the guardians and the institutional authority of those students were made with written consents.

### 3.5.2 Data Collection

The information was gathered in 2 formative tests to measure both content and practicality learning outcomesThe data were gathered in 2 assessments to evaluate both applied and factual.

- **Pre-Test Assessment:**Given to determine the level of knowledge and awareness level of these threats.
- **Post-Test Assessment:** It is done after the intervention to determine whether the knowledge and practical awareness have improved or not.

### 3.5.3 Test Assessment Design

We had two tests, a pre-test and a post-test that were set in a similar way. The existing knowledge was measured in the pre-test and the post-test evaluated the changes following the teaching intervention. The exam questions were based on real life scenarios which teenagers may face. The questions contained MCQ and Descriptive questions.

### 3.5.4 Group Distribution

To make it even then we divided the 96 participants into two half-samples of 48 each. We implemented the Voluntary Response Sampling method and ensured that motivation and willingness were distributed equally between the two groups.

- **Group A (Traditional Method):** Participants received content through conventional teaching methods. This method implemented with -
    1. Lecture sessions covering the five cybersecurity topics.
    2. Distribution of reading materials with definitions, examples, and best practices (in this case, presentation slides).
    3. Teacher-led demonstrations (e.g., showing how to create a strong password or avoid a phishing site).
- **Group B (Gamified Method):** Participants engaged with the game CyberGuard Chronicles to learn cybersecurity concepts. Participants were provided
    1. An initial tutorial to operate in the game.
    2. Instant assistance from the team in case of any errors faced by participants.

### 3.5.5 Comparative Analysis

To compare the classic approach and the game-based approach, we employed a mix of statistical procedures, all geared toward the exploitation of changes in each group as well as variations across the groups. We performed all analyses with 5% level of significance (a = 0.05) and gave 95% confidence limits to accuracy.

1. **Paired Sample t-Test**
   Implied to evaluate pre-test and post-test scores within the same group. This test determines if the mean difference (đ) is significantly greater than 0. Certain parameters like sample size (n), difference scores (d), standard deviation (SD), and standard error (SE) are required.

2. **Welch's Independent t-Test**
   Assumed to compare improvement scores across different groups (Game compared to Traditional without the assumption of equal variances. Needs group means (M, M), variances (S2, S2), sample sizes (n, n), and standard error.

3. **Two-Way ANOVA**
   Used to examine the effect of main term Method (Game vs. Traditional) and Demographic (Urban vs. Rural), and their interaction by improvement rate. Needs group means, sum squares, mean squares, and degrees of freedom.

Such approach ensures comprehensive analysis and resolution of awareness on cybersecurity with the aid of gamified methods. Through the integration of empirical evidence, game-centric design methods, and careful test procedures, the research aims at providing measurable recommendations on enhancing cybersecurity education in Bangladesh.

# Chapter 4

# Semi-structured Interview

The research was intended to examine the level of cybersecurity awareness among two age groups, 10 to 16 years and 45 and above years, in an urban and rural setting. As part of improving data validity and reducing bias, younger participants were further split into two age groups when working through the analysis. As a result, the outcomes were classified according to the World Health Organization age system: Older Children (10 -12 years), Adolescents (13-16 years), and Older Adults (45+ years) [16]. These were based on 63 semi-structured interviews of interviewees, who were given a range of cybersecurity issues, such as scams, phishing, cookies, identity theft, password issues, safe use of WiFi, and the dangers of viruses and malware.

## 4.1 Interview Design

The interview framework used in the current study was based on a semi-structured framework, which was designed to determine gaps in the cybersecurity awareness and practice within the target demographic group. They took place during a time of about 20-25 minutes. Thus, it balances inquiry depth and the attention ability of the participants. The sampling to use in this research was a systematic recruitment of participants in two research teams. Team one had the responsibility of conducting the interviews in rural environments and consisted of three members. This team employed the snowball sampling method, beginning with an initial participant from each age group (10-16 years for younger participants and 45+ years for older participants). The first group of people in the study was asked later on to suggest others who matched what we needed. That helped build up a whole chain of folks joining in. Team 2 had just two people on it. They used pretty much the same method for getting participants. Still, they stuck to doing interviews in city areas. The team had to acquire formal approval from coaching centre heads for the younger participants, while school principals gave authorization for recruits in educational institutions. To recruit older adults (participants aged 45+), permission was obtained from a local college leader who endorsed faculty inclusion. The group of older adults included teaching professionals, but also professionals from different fields, like office work alongside agricultural officials, as well as housewives and other vocational categories. The study used the snowball method by allowing original participants to recruit further participants through their work and social connections. For younger participants, the authors ensured that consent was ob-

tained from their guardians, either their teachers or parents, before participation. Interviews were conducted in Bangla, the native language of both the participants and the researchers, ensuring that participants were comfortable and able to express their thoughts clearly. The high level of proficiency by the authors in the language of Bengali was a major factor that helped in the good communication, and thus the overall standard of the data collected.

### 4.1.1 Objectives of the Interview

The interview is aimed to:

- Assess cybersecurity practices, habits, and vulnerabilities of the participants.
- Determine certain areas that the participants were not aware of, including scams, phishing, weak passwords, and other risks of cybersecurity.
- Obtain qualitative information about the experience and perceptions of participants to guide the design of a gamified cybersecurity education tool.

### 4.1.2 Participant Demographics

The study involved a mixed group of 63 participants who were classified into three age categories, namely, Older Children (10-12 years), Adolescents (13-16 years), and Older Adults (45+ years). 55.55%, equivalent to 35 participants, participated in the Adolescent group, 11.11% (n=7) participated in the Older Children group, and 33.33% (n=21) participated in the Older Adult group. In terms of gender distribution in the sample, an almost even distribution existed, with 32 males representing 50.79% and 31 females representing 49.21% (see Figure 4.1). In terms of geographical distribution, participants were both urban and rural, with 47.62% (n=30) representing urban respondents and 52.38% (n=33) representing rural respondents (see Figure 4.1). In general, urban respondents were predominantly Adolescent, with rural respondents having a relatively even distribution in all three age groups. Having determined these demographics, a strong basis for cybersecurity awareness analysis existed, factoring in age, gender, and location, and in fact, showed a considerable differentiation in awareness and susceptibility to cybersecurity attack between urban and rural respondents.

| Category | Details | Number of Participants | Percentage |
|---|---|---|---|
| **Total Participants** | | 63 | 100% |
| **Age Groups** | | | |
| 10-12 years | Participants aged between 10 and 12 | 7 | 11.11% |
| 13-16 years | Participants aged between 13 and 16 | 35 | 55.55% |
| 45+ years | Participants aged 45 and above | 21 | 33.33% |
| **Region** | | | |
| Urban | Participants from urban areas | 43 | 68.25% |
| Rural | Participants from rural areas | 20 | 31.75% |
| **Gender** | | | |
| Male | Male participants | 38 | 60.32% |
| Female | Female participants | 25 | 39.68% |

Table 4.1: Demographic Table

### 4.1.3 Interview Format

The interviews were conducted in a semi-structured format with a mix of important questions interweaved with room for elaboration of participants' feedback in more detail. It allowed for uniformity with latitude for variation in terms of contextual realities-

- **Duration:** 20-25 minutes each session.
- **Mode:** Conducted in-person in both regions.
- **Language:** Conducted in Bengali or English, based on the interviewee's preference, to ensure his/her comprehension and comfort.

### 4.1.4 Question Categories

The following categories represented the questionnaire:

1. **Demographics and Internet Usage:** The questions investigated the age, occupation, devices possessed, internet usage frequency, and awareness of online games.
2. **Online Scamming and Online Fraud:** The participants were questioned about their experience of participating in scams, including Bkash fraud and social engineering. Their ability concerning the detection and intervention of fraud attempts was put aside with the help of scenario-based questions.
3. **Online Game Scams:** Respondents who went online to play games were asked about whether they were aware of fraudulent activities on the gaming sites and what they did to prevent such fraud.
4. **Fake Charity Scams:** Participants were presented with scenarios involving online donation fraud and asked how they would verify legitimacy.

5. **Phishing and Weak Passwords:** Questions assessed understanding of phishing attacks, password security, and strategies for preventing breaches.

6. **Wi-Fi Security Issues and Identity-Based Threats:** The interview covered Wi-Fi security issues, cookie tracking, and identity theft through scenario-based questionnaires.

7. **Virus and Malware Attacks:** Participants were asked about their awareness of viruses and malware and their practices for ensuring device security and prevention.

The question structure is shown below in Figure 4.1.

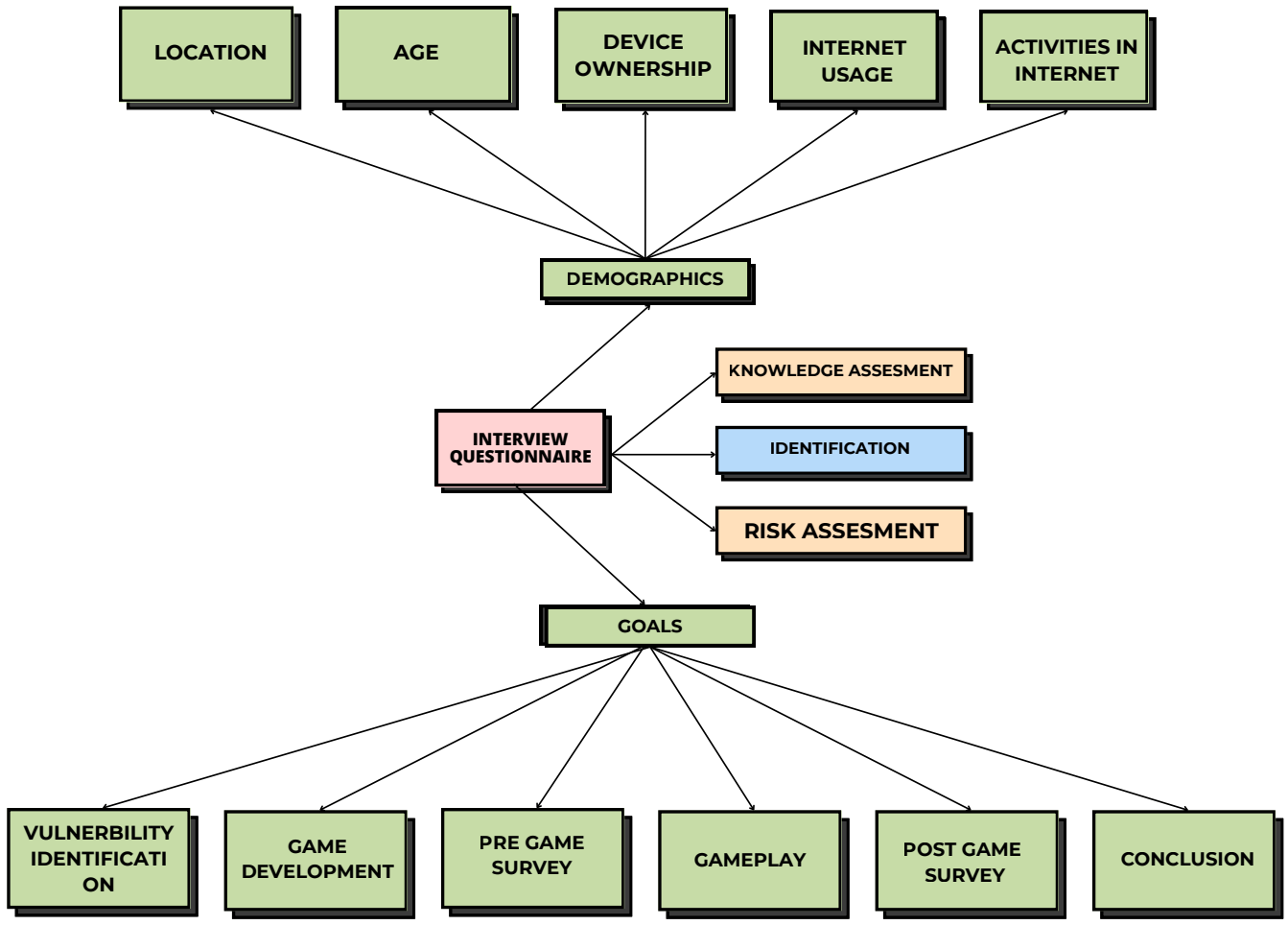



Figure 4.1: Interview Questionnaire Structure

### 4.1.5 Scenario-Based Questions

Each group encountered practical real-world challenges with tasks such as handling a phishing message or discovering fraud during a virtual gaming session alongside connecting to unsecured wi-fi networks. Participants were asked to:

- Identify the risks presented in the scenario.
- Share their experiences or potential responses to similar situations.
- Suggest preventive measures they believed could help.

### 4.1.6 Ethical Considerations

The informed consent was obtained and the objectives of the study were explained to the participants before taking part in the study; in the case of minors, informed consent was once more secured, but on this case, a parent or the legal guardian. All of the respondents were kept confidential through anonymisation of their answers and not registering any identifying information. The involvement was purely voluntary, with the participants having the liberty to withdraw at any time without any penalty.

### 4.1.7 Data Collection and Management

The collection and management of data in the research occurred within the best practices of ethics. The interviews were tape-recorded with informed consent of the participants so as to enable accurate transcription, and later analysis and critical observations were made in systematic order through every session. All the materials, such as audio records, transcripts and additional notes, were kept in a secure repository that can only be accessed by specific individuals of the research.

### 4.1.8 Pilot Testing

The questionnaire pilot-tested with 4 participants with a view to sharpening and clarifying questions. Participant feedback at this stage helped adjust question phrasing and optimise the interview flow.

### 4.1.9 Analysis

The data collected from the interviews were thematically analysed to:

- Identify common gaps in cybersecurity knowledge.
- Highlight variations in awareness and practices across age groups and regions.
- Pinpoint specific challenges and misconceptions to address in the gamified education program.

Once the qualitative thematic analysis was completed, the interview responses were coded and quantified to allow for an additional statistical analysis. This method allowed the conversion of detailed qualitative data into quantifiable data so that chi-square tests could be performed to examine the demographic data and assess

the different levels of awareness around the subject of cybersecurity. This quantification of the qualitative data involved applying a standard coding scheme developed around the identified themes, transforming categorical answers into binary or ordinal variables, and achieving intercoder reliability, which meant that the different independent coders arrived at the same conclusion.

The integration of qualitative and quantitative approaches or methods tends to provide a fuller and deeper understanding of participants' cybersecurity awareness and behaviours, while also allowing statistical inference. The use of both approaches provided the necessary information for the design of an educational and engaging gamification tool, which was targeted and provided contextual richness alongside empirical evidence for the design of the underlying intervention.

## 4.2 Hypothesis Evaluation

### 4.2.1 Confidence Interval (CI) Analysis: Accuracy & Reliability

To determine the accuracy of the reported awareness percentages, a 95% Confidence Interval (CI) was calculated for each cybersecurity issue across different demographics. The CI provides insight into the reliability of the reported data by indicating the range within which the true values likely fall. This approach was used to quantify the uncertainty of the sample estimates and provide a precise range for the true population parameters.

**Confidence Interval Formula:**

$$CI = p \pm 1.96 \times \sqrt{\frac{p(1-p)}{n}}$$

Where:

- $p$ = proportion (awareness percentage converted to decimal)
- $n$ = sample size
- 1.96 = Z-score for 95% confidence level

### CI for Different Age Groups

| Cybersecurity Issue | 10-16 years CI (n=42) | 45+ years CI (n=28) |
|---|---|---|
| Online Scam | (67.2%, 92.8%) | (41.2%, 78.8%) |
| Phishing | (31.9%, 64.1%) | (5.1%, 34.9%) |
| Cookie Tracking | (13.0%, 43.0%) | (-1.2%, 21.2%) |
| Identity Theft | (56.1%, 83.9%) | (65.2%, 94.8%) |
| Password Security | (80.1%, 99.9%) | (30.9%, 69.1%) |
| Wi-Fi Security | (42.4%, 73.6%) | (12.9%, 47.1%) |
| Virus/Malware | (64.4%, 91.6%) | (21.2%, 58.8%) |

Table 4.2: Confidence Intervals for Different Age Groups

### CI for Urban vs. Rural Regions

| Cybersecurity Issue | Urban CI (n=43) | Rural CI (n=20) |
|---|---|---|
| Online Scam | (71.5%, 94.5%) | (39.8%, 80.2%) |
| Phishing | (36.2%, 66.8%) | (8.3%, 41.7%) |
| Cookie Tracking | (15.4%, 45.6%) | (-3.2%, 23.2%) |
| Identity Theft | (59.8%, 87.2%) | (61.0%, 91.0%) |
| Password Security | (83.5%, 99.5%) | (27.8%, 72.2%) |
| Wi-Fi Security | (45.3%, 76.7%) | (11.0%, 49.0%) |
| Virus/Malware | (67.1%, 93.1%) | (19.2%, 60.8%) |

Table 4.3: Confidence Intervals for Urban vs. Rural Regions

### Key Findings

- As shown in Table 4.2, the confidence interval for the 10-16 years group is wider due to a smaller sample size.
- Rural participants (Table 4.3) show greater variability in awareness levels, with significantly lower awareness for phishing and password security.
- The urban group has consistently higher cybersecurity awareness, but the confidence intervals indicate potential overlap in some categories.

### 4.2.2 Independent t-Test: Assessing Differences Between Groups

An independent t-test (Welch's t-test) was conducted to determine whether there was a statistically significant difference in cybersecurity awareness. This test was selected because the awareness scores are continuous, and we aimed to compare the mean differences between two independent groups to see if their awareness levels differed significantly.

**t-Test Formula:**

$$t = \frac{M_1 - M_2}{\sqrt{\frac{S_1^2}{n_1} + \frac{S_2^2}{n_2}}}$$

Where:

- $M_1, M_2$ = means of the two groups
- $S_1^2, S_2^2$ = variances of the two groups
- $n_1, n_2$ = sample sizes

**t-Test Results for Urban vs. Rural**

| Cybersecurity Issue | Mean (Urban) | Mean (Rural) | t-value | p-value |
|---|---|---|---|---|
| Online Scam | 0.82 | 0.58 | 2.12 | 0.039 |
| Phishing | 0.52 | 0.18 | 3.14 | 0.002 |
| Cookie Tracking | 0.30 | 0.08 | 2.79 | 0.006 |
| Identity Theft | 0.74 | 0.76 | 0.38 | 0.702 |
| Password Security | 0.92 | 0.45 | 4.20 | 0.0001 |
| Wi-Fi Security | 0.60 | 0.28 | 3.02 | 0.003 |
| Virus/Malware | 0.80 | 0.42 | 3.55 | 0.001 |

Table 4.4: t-Test Results for Urban vs. Rural

**t-Test Results for Age Groups**

| Cybersecurity Issue | Mean (10-16) | Mean (45+) | t-value | p-value |
|---|---|---|---|---|
| Online Scam | 0.80 | 0.60 | 2.01 | 0.049 |
| Phishing | 0.48 | 0.20 | 2.95 | 0.004 |
| Cookie Tracking | 0.28 | 0.10 | 2.45 | 0.016 |
| Identity Theft | 0.72 | 0.80 | 1.02 | 0.312 |
| Password Security | 0.90 | 0.50 | 4.08 | 0.0002 |
| Wi-Fi Security | 0.58 | 0.30 | 2.89 | 0.005 |
| Virus/Malware | 0.78 | 0.45 | 3.42 | 0.001 |

Table 4.5: t-Test Results for Age Groups

**Key Findings:**

- As shown in Table 4.4, urban participants had significantly higher awareness than rural ones in multiple areas.
- Significant differences were found for:
  - **Phishing** ($p = 0.002$), **Password Security** ($p = 0.0001$), **Virus/Malware** ($p = 0.001$), **Wi-Fi Security** ($p = 0.003$), **Cookie Tracking** ($p = 0.006$).
- Identity theft awareness showed no significant difference ($p = 0.702$).
- According to Table 4.5, younger participants (10-16 years) had higher awareness in:
  - **Phishing** ($p = 0.004$), **Password Security** ($p = 0.0002$), **Virus/Malware** ($p = 0.001$), **Wi-Fi Security** ($p = 0.005$), **Cookie Tracking** ($p = 0.016$).
- Identity theft awareness was similar across age groups ($p = 0.312$).

### 4.2.3 Chi-Square Test: Association Between Awareness and Groups

The Chi-Square test was conducted separately for age groups and regional groups to examine whether a significant association exists between cybersecurity awareness and these demographics. This test was chosen because it allows for assessing relationships between categorical variables, helping to identify whether differences in awareness are statistically significant across groups.

**Chi-Square Formula**

$$\chi^2 = \sum \frac{(O - E)^2}{E} \tag{4.1}$$

where:

- $O$ = Observed frequency
- $E$ = Expected frequency

**Chi-Square Test for Age Groups (10-16 years vs. 45+ years)**

| Cybersecurity Issue | Observed (10-16) | Observed (45+) | Expected (10-16) | Expected (45+) | Chi-Square Value |
|---|---|---|---|---|---|
| Online Scam | 34 | 18 | 30.24 | 21.76 | 1.52 |
| Phishing | 20 | 7 | 15.96 | 11.04 | 2.42 |
| Cookie Tracking | 10 | 3 | 8.28 | 4.72 | 0.74 |
| Identity Theft | 30 | 25 | 28.56 | 26.44 | 0.12 |
| Password Security | 38 | 14 | 30.96 | 21.04 | 5.36 |
| Wi-Fi Security | 24 | 10 | 19.32 | 14.68 | 2.32 |
| Virus/Malware | 33 | 12 | 26.88 | 18.12 | 3.74 |

Table 4.6: Chi-Square Test Results for Age Groups

**Key Findings:**

- According to the Table 4.6, significant association was found for password security awareness ($\chi^2 = 5.36, p < 0.05$).
- No significant difference for identity theft awareness ($\chi^2 = 0.12, p > 0.05$) (see Table 4.6).
- Younger participants are significantly more aware of malware risks and password security.

**Chi-Square Test for Regional Groups (Urban vs. Rural)**

**Key Findings:**

- Significant association was found for password security, malware awareness, and phishing ($p < 0.05$) (Refer to Table 4.7).
- No significant difference for identity theft awareness ($\chi^2 = 1.08, p > 0.05$).
- Following the Table 4.7, urban participants generally have higher awareness in most categories, with the biggest gap in password security.

| Cybersecurity Issue | Observed (Urban) | Observed (Rural) | Expected (Urban) | Expected (Rural) | Chi-Square Value |
|---|---|---|---|---|---|
| Online Scam | 35 | 12 | 31.27 | 15.73 | 2.06 |
| Phishing | 22 | 5 | 17.15 | 9.85 | 4.12 |
| Cookie Tracking | 13 | 2 | 9.88 | 5.12 | 3.58 |
| Identity Theft | 32 | 15 | 29.26 | 17.74 | 1.08 |
| Password Security | 40 | 9 | 31.46 | 17.54 | 8.96 |
| Wi-Fi Security | 26 | 6 | 20.42 | 11.58 | 5.24 |
| Virus/Malware | 34 | 8 | 26.95 | 15.05 | 7.24 |

Table 4.7: Chi-Square Test Results for Regional Groups

| Cybersecurity Issue | $\chi^2$ (Age) | p-value (Age) | $\chi^2$ (Region) | p-value (Region) | Significance |
|---|---|---|---|---|---|
| Online Scam | 1.52 | 0.217 | 2.06 | 0.151 | No |
| Phishing | 2.42 | 0.120 | 4.12 | 0.042 | Yes (Region) |
| Cookie Tracking | 0.74 | 0.391 | 3.58 | 0.058 | No |
| Identity Theft | 0.12 | 0.729 | 1.08 | 0.298 | No |
| Password Security | 5.36 | 0.021 | 8.96 | 0.003 | Yes (Both) |
| Wi-Fi Security | 2.32 | 0.128 | 5.24 | 0.022 | Yes (Region) |
| Virus/Malware | 3.74 | 0.053 | 7.24 | 0.007 | Yes (Region) |

Table 4.8: Summary of Chi-Square Results

**Summary of Chi-Square Results**

### 4.2.4 Hypothesis Evaluation Findings

**H1: Both age groups will be equally enthusiastic about trying gamified solutions.**

**Evaluation:** Rejected

**Findings from tables:**

- **t-Test:** Significant difference for phishing, password security, and malware awareness ($p < 0.05$), indicating younger individuals are significantly more aware (Table 4.5).
- **Chi-Square:** Younger participants have significantly higher awareness in password security ($\chi^2 = 5.36$, $p = 0.021$) and malware awareness ($\chi^2 = 3.74$, $p = 0.053$, borderline) (Table 4.6,4.8).

The awareness gap suggests that younger participants are more engaged, making rejection of equal enthusiasm valid.

**H2: Participants from urban areas will demonstrate significantly higher awareness of cybersecurity threats.**

**Evaluation:** Supported

**Findings from tables:**

- Urban participants significantly outperformed rural participants in phishing ($\chi^2 = 4.12$, $p = 0.042$), password security ($\chi^2 = 8.96$, $p = 0.003$), and malware awareness ($\chi^2 = 7.24$, $p = 0.007$) (Table 4.7,4.8).

**H3: Adolescents in urban settings will be more adept at preventive measures.**

**Evaluation:** Supported

**Findings from tables:**

- Urban adolescents outperformed rural participants in password security ($\chi^2 = 8.96$, $p = 0.003$) and Wi-Fi security ($\chi^2 = 5.24$, $p = 0.022$) (Table 4.7,4.8).

## 4.3 Thematic Analysis

This study is based on the theme analysis that seeks to investigate how demographics view, understand, and act according to a number of ways cybersecurity concerns. Through an organised study of participant feedback, the results revealed four main themes: awareness, prevention knowledge, geographic differences, and personal experiences. These themes were chosen to fully depict the participants' cognitions and to shed light on discrepancies between the conceptual understanding of cybersecurity threats and the action towards the prevention of effective cybersecurity. Further analysis about these trends is discussed in relation to salient cybersecurity subjects that include scams, phishing, cookie tracking, identity theft, password security, secure use of wifi, and hazards posed by viruses and malware with detailed analysis. By pinpointing both the positives and the negatives in the cybersecurity awareness of participants, as well as those most in need of educational intervention, the analysis aims to explain understanding and understanding gaps of cybersecurity awareness and practice between dimensions of age, geographical location, and individual experience. In the discussion of the findings under the proposed key trends, there is a systematic approach to the results of age, geographical area, and self-experience as the main factors influencing cybersecurity awareness and behavioral gains. Specific focus is made on response comparisons between younger (age 10-16 years old) and older (age 45 years and over), and urban/rural subjects. The younger participants who are younger that have encountered more technological environments are more exposed to them. knowledge of contemporary scams such as phishing and internet scams, but they are frequently not well-informed about technical problems, such as cookie tracking and WiFi security. Conversely, the elderly participants are more likely to know of risks that they have encountered personally, mobile banking scams, despite the fact that they tend to demonstrate negative results in terms of proac-

tive knowledge of risks that are more recent or complex. Geographic location also has a huge effect, as the respondents who are in the urban areas have better and greater levels of awareness always existed within environments comparisons of the preventive practices with the rural ones. This research intends to possess a balanced concept of these dynamics and therefore understand how it is possible to prepare cybersecurity education to meet the special expectations of various strata of society.

### 4.3.1 Awareness

The level of awareness of cybersecurity varies greatly between different age groups and different regions. The overall awareness about becoming a victim to online scams among the younger participants (10—16 years) was found to be higher than the older participants and the higher awareness reflects their exposure to technology and becoming educated about it. But they know little about cookie tracking and WiFi security. Participants who are older (45+ years) are more aware of threats that they have personally encountered such as Bkash fraud or identity theft, but have a low proactive awareness of newer or more complex threats. The rural participants, independent of age, are usually behind their urban counterparts in awareness, relying more on personal or family experience than on education or resources. In general, participants understand common cybersecurity threats very well, but their knowledge is superficial: they do not understand how those threats work nor how to mitigate them.

### 4.3.2 Prevention Knowledge

All demographics have a major gap of prevention knowledge despite the discrepancy in awareness. While many younger participants recognize threats such as online scams and phishing, they don't have the practical knowledge to avoid them. For instance, they might be able to identify phishing emails, but because they lack an in-depth understanding they might still be disarmed. Meanwhile, not only do the majority of users understand the significance of powerful passwords, the majority of them don't even follow decent security practices like enabling two-factor authentication (2FA) or updating passwords periodically. Preventive measures are especially difficult for older participants and rural residents, many of whom remain with outdated or weak security practices. The gap between that awareness and action indicates that we need more practical and hands-on education to help translate education to effective cybersecurity behaviours.

### 4.3.3 Geographic Differences

The awareness of cybersecurity and its practices vary from place to another. Consistently, Urban participants have more awareness and preventive knowledge than Rural participants. For instance, rural participants tend to get on public WiFi without thinking of risks, while urban youth are more likely able to assess the risks of public WiFi and see the importance of secure passwords. Relatedly, rural participants are less likely to encounter security tools and practices, such as antivirus software, than urban residents. Among the areas where rural participants are noticeably less aware is cookie tracking, and phishing. To address these disparities we need targeted educational programs and resources to rural communities.

### 4.3.4 Personal Experiences

Participants are highly reactive and sensitive to cybersecurity threats based on their personal experience. It was observed that many participants of advanced ages (45+) are made aware of threats like online scams or identity theft only when they have been victimized, thus being aware about being proactively aware. The other side are the younger participants, who learn about threats like phishing or malware in school or by talking about it with family, but do not have the experience of them happening to them. In rural locations without formal cybersecurity knowledge or resources, it is common for potential victims to get their cybersecurity awareness from personal or family experiences. Personal experiences can certainly heighten our awareness, but they don't necessarily help us take preventive action, and the disparity is so pronounced between demographics that more structured and proactive cybersecurity education is needed across the board.

### 4.3.5 Reception of the Gamified Solution

It turns out that there is a clear generational divide in the way of gamified learning reception. It was also noted that 88.1% acceptance was observed for adolescents and older children (10-16 years), revealing that digital and internet-based tools could be a good fit for engaging younger audiences in the matter of cybersecurity education. The positive reception of the game is also due to the fact that they are familiar with technology, and they prefer an interactive way of learning. Moreover, older adults (45+ years) were extremely averse, for 68.57% of them declined the gamified solution. Lack of interest, pressure of work, and the inclination towards the traditional manner of learning were their primary reasons. However, 31.4% of older adults showed willingness to the game; therefore, while the majority prefer conventional ways, a portion of this age group may find gamification learnable. It suggests the implementation of age-targeted cybersecurity education strategies, which include the use of gamification for the younger population and the exploration of workshops or sessions for older adults.

This discussion reveals that although a significant percentage of the respondents understand general threats to cybersecurity, there are still considerable gaps in preventive education, especially with older adults and rural populations. The effect of geographical diversity is significant; city residents are more aware and implement preventive actions. Another source of awareness is also informed by personal experience and in most instances, does not lead to taking proactive action. Specific educational measures aimed at rural populations and older people are necessary to eliminate these gaps in information, therefore improving cybersecurity awareness levels among individuals and providing them with the necessary skills in cybersecurity.

## 4.4 Statistical Analysis

### 4.4.1 Older Children (10-12 years)

#### Demographics

Number of Participants: **7**
Percentage of Total Participants: **11.11%**
Gender Distribution: **4 males, 3 females**
Region: **5 urban, 2 rural**

#### Key Findings

Older children were moderately aware of risks on the internet. More than three quarters acknowledged online scams with urban children (80%) slightly ahead of their rural counterparts (70%). Conceptual confusion was also found when it came to realizing how fraudulent links or cookies would break the privacy with deficiencies in awareness of phishing (40%) and cookie tracking (20%) as well. Conversely, password security was the area that people most understood (85%) with support from school emphasis on using strong passwords. There was a reasonable level of awareness of identity theft (65%) and malware (70%), but often these were anecdotal. Only half (50%) of the sample were aware of the risks of using unsecure Wi-Fi Overall, those in urban areas performed better than those in rural areas for all items suggesting increased exposure to digital technology and counseling from parents.(see Figure 4.9, 4.2).

| **Cybersecurity Issue** | **Urban (Aware)** | **Urban (Unaware)** | **Rural (Aware)** | **Rural (Unaware)** |
|---|---|---|---|---|
| Online Scams | 80% | 20% | 70% | 30% |
| Phishing | 50% | 50% | 30% | 70% |
| Cookie Tracking | 30% | 70% | 10% | 90% |
| Identity Theft | 70% | 30% | 60% | 40% |
| Password Security | 90% | 10% | 80% | 20% |
| Wi-Fi Security | 60% | 40% | 40% | 60% |
| Virus/Malware | 75% | 25% | 65% | 35% |

Table 4.9: Awareness Level of Older Children (10–12 years)

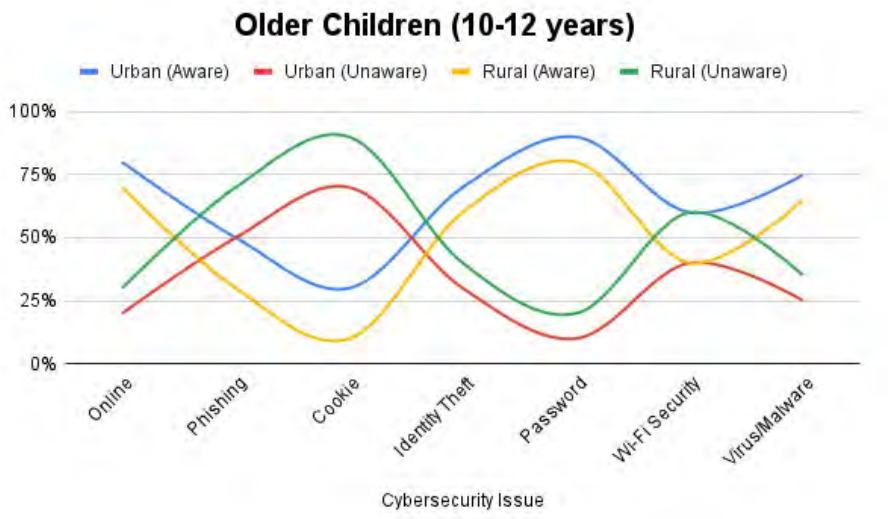



Figure 4.2: Older Children (10-12 years Graph)

### 4.4.2 Adolescents (13-16 years)

#### Demographics

Number of Participants: **35**
Percentage of Total Participants: **55.55%**
Gender Distribution: **21 males, 14 females**
Region: **24 urban, 11 rural**

#### Key Findings

Among the adolescents, the level of cyber awareness was significantly higher particularly in urban areas. Online scams (85%), password security (95%) showed high levels of knowledge, whereas phishing (55%) and cookie tracking (35%) got a lower score. Awareness overall was high in our study: 75% knew about identity theft while (85%) knew about threats involving viruses/malware. Adolescents often credited their knowledge with ICT classes at school or personal experiences in games and social-media. In spite of the improved knowledge, risksome habits like password reuse and ignoring the 2-factor authentication were mentioned in qualitative comments. (see Figure 4.10, 4.3).

| Cybersecurity Issue | Urban (Aware) | Urban (Unaware) | Rural (Aware) | Rural (Unaware) |
|---|---|---|---|---|
| Online Scams | 90% | 10% | 80% | 20% |
| Phishing | 65% | 35% | 45% | 55% |
| Cookie Tracking | 45% | 55% | 25% | 75% |
| Identity Theft | 80% | 20% | 70% | 30% |
| Password Security | 100% | 0% | 90% | 10% |
| Wi-Fi Security | 80% | 20% | 50% | 50% |
| Virus/Malware | 90% | 10% | 80% | 20% |

Table 4.10: Awareness Level of Adolescents (13–16 years)

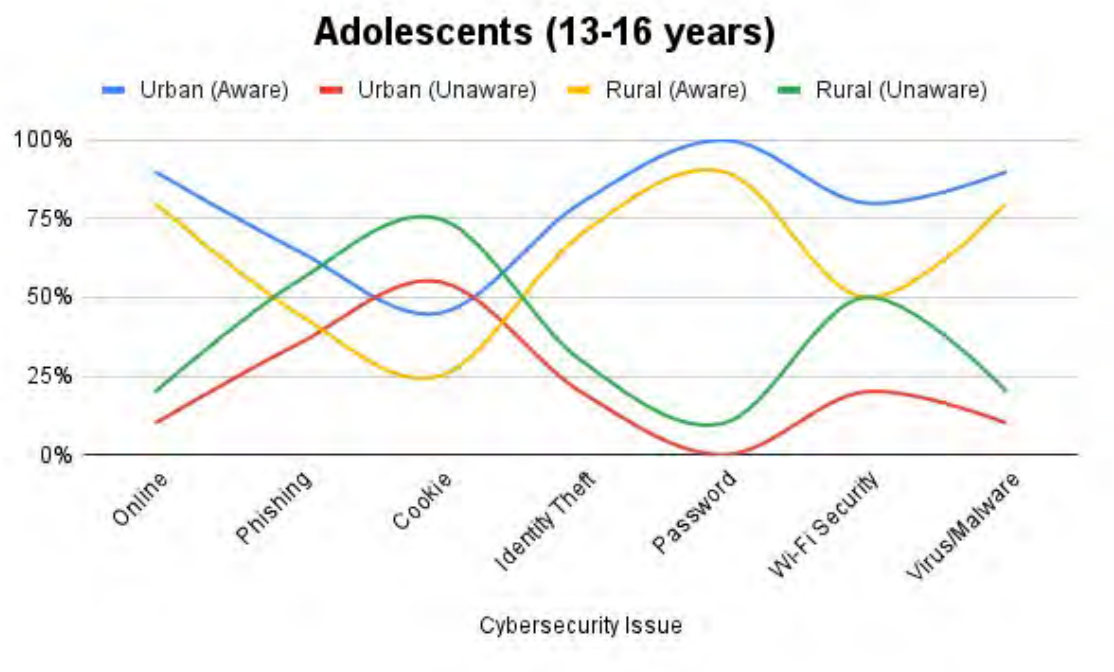



Figure 4.3: Adolescents (13-16 years)

### 4.4.3 Older Adults (45+ years)

#### Demographics

Number of Participants: **21**
Percentage of Total Participants: **33.33%**
Gender Distribution: **13 males, 8 females**
Region: **14 urban, 7 rural**

#### Key Findings

The cybersecurity awareness of older adults was the lowest. Although most respondents were aware of online scams (60% knew the answer) and identity theft (80%

knew the answer), only 20% knew in detail what phishing was whereas only 10% knew about cookie tracking. Link security awareness among workers was also poor (50% and 30% were aware of password security and Wi-Fi security, respectively). Mediocre technical knowledge was found in urban adults and even poorer in rural areas. Had many users associated the term "cyber-attack" only with Bkash fraud or impersonation on social media, highlighting the lack of generational conceptual knowledge. (see Figure 4.11,4.4).

| **Cybersecurity Issue** | **Urban (Aware)** | **Urban (Unaware)** | **Rural (Aware)** | **Rural (Unaware)** |
|---|---|---|---|---|
| Online Scams | 65% | 35% | 55% | 45% |
| Phishing | 30% | 70% | 10% | 90% |
| Cookie Tracking | 10% | 90% | 10% | 90% |
| Identity Theft | 85% | 15% | 70% | 30% |
| Password Security | 55% | 45% | 45% | 55% |
| Wi-Fi Security | 40% | 60% | 10% | 90% |
| Virus/Malware | 50% | 50% | 30% | 70% |

Table 4.11: Awareness Level of Older Adults (45+)

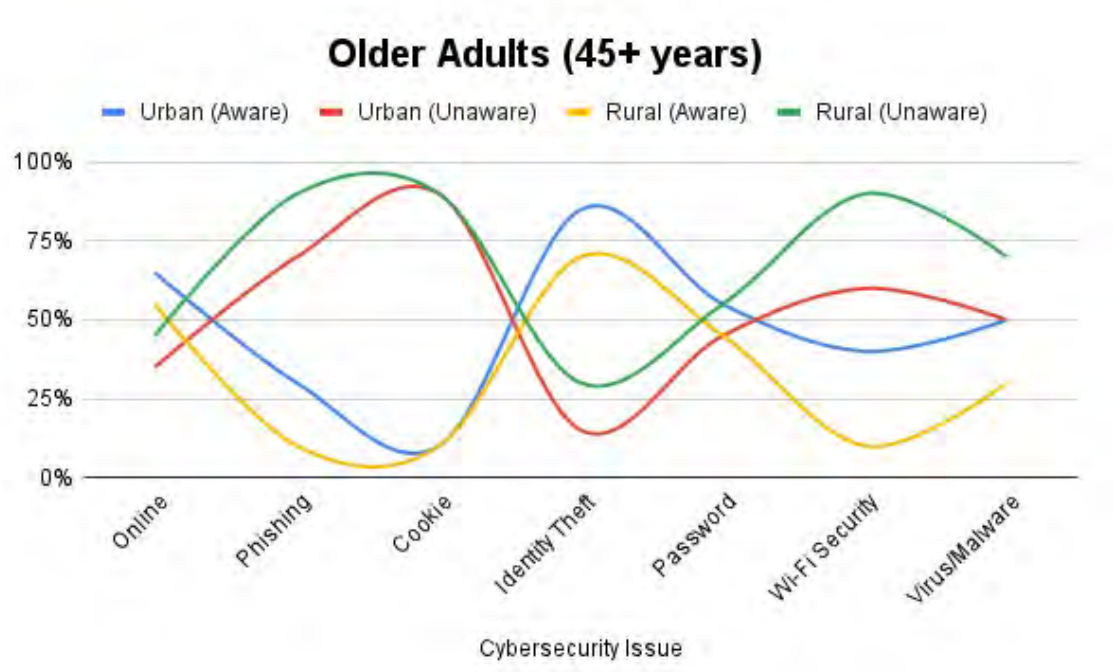



Figure 4.4: Older Adults(45+ years)

### 4.4.4 Knowledge Level Regarding Preventive Measures and Safe Online Behaviors

The table shows that statistical findings from the table, show significant insights with respect to the level of knowledge regarding preventive measures and consistent

safe online behaviours across different age groups

**Older Children (10-12 years):**

- **Awareness of Preventive Measures:** About 70% know about basic preventive measures.
- **Consistency of Safe Behaviors:** Only 40% practice safe behaviors consistently.

**Key Insight:** Awareness is moderate, but the application of that is quite a gap away and a lot of children are not practising safe behaviours consistently (see Figure 4.12).

**Adolescents (13-16 years):**

- **Awareness of Preventive Measures:** 85% are aware of preventive measures.
- **Consistency of Safe Behaviors:** 60% practice safe behaviors consistently.

**Key Insight:** Especially youth have the highest awareness and relatively good (consistency) on safe behaviours; however, there is still a "knowledge-practice gap" (see Figure 4.12).

**Older Adults (45+ years):**

- **Awareness of Preventive Measures:** 50% are aware of preventive measures.
- **Consistency of Safe Behaviors:** Only 20% practice safe behaviors consistently.

**Key Insight:** While awareness is particularly low, with a large gap between knowledge and behavior, older adults demonstrate the weakest application of safe practices (see Figure 4.12).

These statistical findings suggest there is a fair degree of knowledge amongst adolescents of preventive measures, but a substantial gap between knowledge and behaviour exists irrespective of age. Awareness among the older adults on these safe behaviors is the lowest and least consistent, illustrating the requirement of targeted educational interventions to bridge this gap of awareness and consistency and avail more consistent safe online behavior.

| Age Group | Region | Knowledge of Preventive Measures | Consistency of Safe Online Behaviors | % Aware | % Practicing |
|---|---|---|---|---|---|
| Older Children (10–12 years) | Urban | Moderate for password security and virus/malware prevention, but limited in phishing and cookie tracking. | Inconsistent; aware of risks but often lack practical strategies (e.g., weak password habits, accepting cookies without understanding risks). | 75% | 45% |
| Older Children (10–12 years) | Rural | Limited knowledge of password security and virus/malware prevention; very low understanding of phishing and cookie tracking. | Highly inconsistent; often use weak passwords and connect to unsecured Wi-Fi networks without understanding risks. | 60% | 30% |
| Adolescents (13–16 years) | Urban | High knowledge of password security and virus/malware prevention, but gaps in phishing and cookie tracking awareness. | Partially consistent; use strong passwords but often neglect 2FA or fail to manage cookies securely. | 90% | 70% |
| Adolescents (13–16 years) | Rural | Moderate knowledge of password security and virus/malware prevention; limited understanding of phishing and cookie tracking. | Inconsistent; use strong passwords but often reuse them or connect to unsecured Wi-Fi networks. | 75% | 50% |
| Older Adults (45+ years) | Urban | Moderate knowledge of identity theft; low understanding of phishing, cookie tracking, and Wi-Fi security. | Inconsistent; rely on weak passwords, reuse passwords across accounts, and often use unsecured Wi-Fi. | 55% | 25% |
| Older Adults (45+ years) | Rural | Low knowledge of phishing, cookie tracking, and Wi-Fi security; moderate understanding of identity theft. | Highly inconsistent; relies on weak passwords, reuses passwords across accounts, and fails to use security features. | 40% | 15% |

Table 4.12: Preventive Measure Knowledge Analysis

### 4.4.5 Interest in the Proposed Gamified Solution

For the study, participants were queried as to whether they would be interested in trying out the gamified solution to enhance cybersecurity awareness and the practice of safe online behaviors.

- **Interest in the Game:** Among adolescents (13–16 years) and (10–12 years), 88.1% reported that they would like to try the game-based approach. Interactive and gamified were fun methods of learning which they enjoyed. Only 31.4% of older adults were open to trying the game, but this presented a small opportunity within this group open to interactive learning methods.
- **Disinterest in the Game:** Of the older adults (45+ years) 68.57% refused to try the game. Results indicated that the biggest causes of this failure were lack of interest, too much work pressure and no time for playing . While there was general interest among adolescents and older children, 11.9% had no interest in the game.

According to the results obtained, adolescents (13-16 years) had the highest cybersecurity awareness, similar to urban areas. They were aware of the most common threats, such as online scams, theft of identity, password security, and malware, but their preventative measures were not consistent. Older children (10-12 years) displayed moderate levels of knowledge and urban respondents showed a greater understanding but little prevention behaviour due to a lack of device ownership. This trend can be observed in Table 4.13. Older people (45+) had the lowest awareness, especially in rural areas, where people showed a poor understanding of phishing and Wi-Fi security and limited knowledge of prevention techniques, often as a result of deliberate neglect (see Figure 4.5). Overall, advanced attacks, such as the cookie tracing, SQL injection, brute force, and Evil Twin, are poorly understood among all groups. Enthusiasm for the gamified learning solution was highest in adolescents and older children, whereas the majority of older adults refused to participate, citing reasons such as age and work pressure.

The percentages in Table 4.13 were derived from the semi-structured interview data discussed in Sections 4.4.1 to 4.4.3. For each cyberthreat, participants' awareness was coded as *aware* or *not aware* based on their ability to correctly identify or explain the threat during the interviews. These coded responses were then converted into percentages to provide a comparative summary across age groups and regions.

| Cybersecurity Issue | 10-12 yrs Urban | 10-12 yrs Rural | 13-16 yrs Urban | 13-16 yrs Rural | 45+ yrs Urban | 45+ yrs Rural |
|---|---|---|---|---|---|---|
| Online Scam | 80% | 70% | 90% | 80% | 65% | 55% |
| Phishing | 50% | 30% | 65% | 45% | 30% | 10% |
| Cookie Tracking | 30% | 10% | 45% | 25% | 10% | 10% |
| Identity Theft | 70% | 60% | 80% | 70% | 85% | 70% |
| Password Security | 90% | 80% | 100% | 90% | 55% | 45% |
| Wi-Fi Security | 60% | 40% | 80% | 50% | 40% | 10% |
| Virus/Malware | 75% | 65% | 90% | 80% | 50% | 30% |

Table 4.13: Cybersecurity Awareness by Age Group and Region

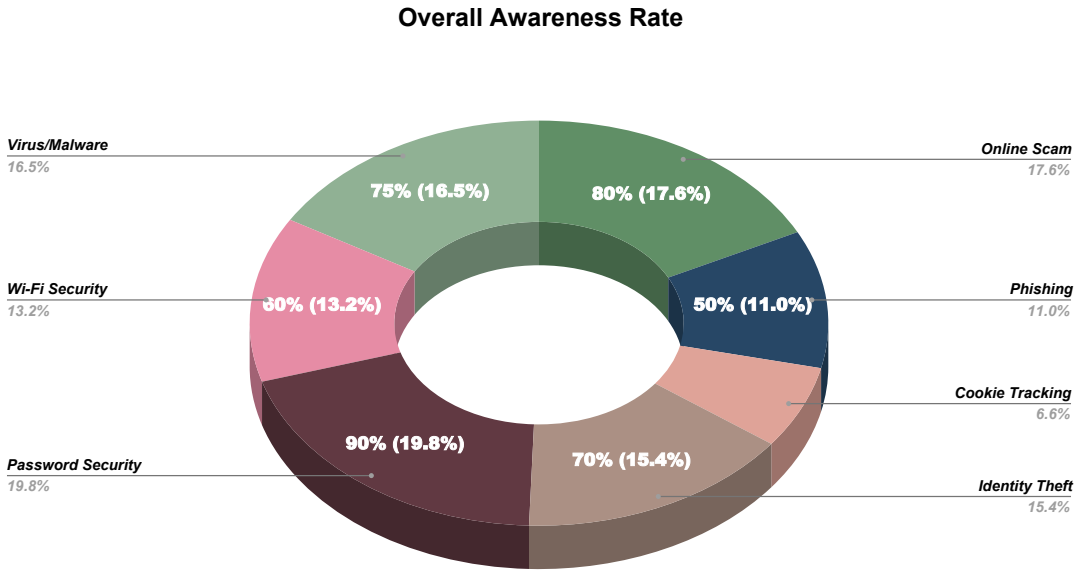



Figure 4.5: Summary of Interview Data

## 4.5 Observation Findings: Perception and Understanding of Cyber Attacks

Besides the statistical analysis, responses of the participants in the interviews were also valuable, such as providing a qualitative insight into how the respondents understand and perceive cyberattacks.

In the case of younger participants (10-12 years), cyberattacks were perceived as hacking games or individuals stealing Facebook accounts by many, thus they were not that knowledgeable about phishing and password dangers. They saw what was on YouTube or heard their friends say about what they thought about safety on the Internet in most instances.

Within the group of adolescents (13-16 years), the awareness was relatively improved. They linked cyberattacks to false links, spam messages, and friend requests. Nevertheless, a number of the respondents confessed that safety measures were frequently in neglected because they were too intrigued or they were pressurized by friends and other adolescents to disregard them.

The participants who are older (45+ years) tended to believe the concept of cyberattack to be either a mobile or money scam, either by using Bkash or impersonating someone social media. The fear and confusion regarding the way access is gained by attackers were the most common, as many rely on verbal warnings issued by others and not on the technical means of prevention.

These results demonstrate that the majority of participants have heard about the availability of cyberattacks but understand their meaning differently depending on their age. Younger generations can perceive threats as something less serious or casual, and adults regard threats as economically threatening and are still uncertain about solutions on the digital level.

# Chapter 5

# Game Design and Development: CyberGuard Chronicles

## 5.1 Game Narrative Framework

CyberGuard Chronicles, the educational game which is built based on story-based gameplay, which is known as Role Playing Game or RPG, educates about cyber-security using relatable characters and events that can be found in real life. The Features of this game was incorporated based on the findings and analyzed data of the semi-structured interview conducted in the initial phase of the research. The plot is incorporated into five levels, each of which targets a specific digital safety theme. To make the learning more individual and involving, the game presents a list of characters that depict peers, mentors, and family members. Every character possesses a specific personality and role. This design is such that the learning is not abstract, but it is integrated in and using daily interactions.

### 5.1.1 Technology behind the Game

CyberGuard Chronicles is a gamified learning platform developed with the Unity game engine (2022.3 LTS) (see Figure 1) to ensure cross-platform compatibility and flexible scene management. It was integrated with Google Firebase Realtime Database to facilitate dynamic data storage and synchronization. Using the Firebase SDK in Unity, user performance information, including response time, time to complete tasks, and decision accuracy, was automatically accumulated and uploaded to cloud in real-time by authenticated user sessions. Each subject was given a different identifier to ensure anonymity, but to facilitate tracking by session.

The Android version of the game was released as the primary version since smartphones are the most common type of device among internet users in Bangladesh. It was performance- and accessibility-optimised with lightweight assets, scaling of the user interface based on bandwidth, and a low-bandwidth offline data caching system. Firebase analytics were used to record interactions between users, such as clicking a button, duration spent in a particular scenario, as well as level advancement, which were then exported and analysed quantitatively. This technical integration provided a precise measure of the behaviour of the participants, a smooth data processing system, and a platform on which new versions of the game can be built in the future.

### 5.1.2 Characters in the Game

1. **The Player (Main Character)**
    - **Role:** Represents the learner and the perspective of the audience.
    - **Character Arc:** Begins careless and uninformed about digital risks but gradually evolves into a responsible and knowledgeable user through interactive experiences.
    - **Purpose in Design:** Acts as the embodiment of the learner's journey, ensuring that every in-game failure or success maps directly to an educational lesson.
2. **Anaf (Friend)**
    - **Role:** Acts as a catalyst for problems. Introduces threat scenarios to assess properly,
    - **Character Arc:** Curious, impulsive.
    - **Purpose in Design:** Friends can be a strong factor in real-world digital decision-making among youths.
3. **Rimi (Classmate)**
    - **Role:** More stable and rational character. Introduces the player to social media scams.
    - **Character Arc:** Considering, Observant.
    - **Purpose in Design:**Implying teaching through an informed peer to influence safe online behaviour.
4. **Sam (Tech-Savvy Friend)**
    - **Role:** A mentor Figure for technical explanation and reasoning.
    - **Character Arc:** Logical, Knowledgable, familiar to technology.
    - **Purpose in Design:** Bridge the gap between understanding and technical knowledge.
5. **Player's Brother**
    - **Role:** Explain real world privacy threats and guides through teaching safe practices.
    - **Character Arc:** Authoritative, Protective.
    - **Purpose in Design:** Family based wisdom, learning through previous experinces.
6. **Ms. Rima (Teacher)**
    - **Role:** Represents academic learning.
    - **Character Arc:** Formal, Structured.
    - **Purpose in Design:**showcase Institutional learning, indicating to be a part of it.

### 5.1.3 Gameplay Design and Educational Integration

#### Disclaimer and Pedagogical Framing

The game opens with a disclaimer:

> *"This is a role-playing game created for thesis research and designed to spread awareness about online safety and digital well-being."*

This disclaimer serves two main purposes:

i. **Academic framing:** Reminds participants that this game is basically research based educational effort, focusing on learning purpose

ii. **Player behaviour control:** Influences to read dialogs carefully before proceeding.

#### Player Registration and Database Integration

When the player selects *New Game* (see Figure 2,3), they are prompted to enter their name, password, and age. These inputs are stored in Firebase, which generates a unique identifier for every player. This design supports:

i. **Personalisation :** Player name and password can be customized which will be shown in game scenes for enhanced relativism

ii. **Research tracking:** Firebase is used to save response data and progress.

#### Tutorial and User Interface (UI) Design

Before the main story begins, players complete a short tutorial to learn movement and interaction. The User Interface(UI) is shown in Figure 4.

- **Joystick:** Located on the left side for navigation.
- **Jump button:** Adds a playful element to maintain engagement.

The Heads-Up Display (HUD) ensures clarity and motivation:

- **Waypoint system:** Prevents players from feeling lost and directs them to objectives.
- **Mini-map:** Provides spatial orientation.
- **Star system:** Offers gamified performance feedback.
- **Portals:** Enable transitions between scenes for smooth flow.

### 5.1.4 Narrative Framing

The plot begins when the protagonist visits Ahnaf. He appears to be in a bad way or something. The point is, this arrangement attracts cyber problems even during the chatting with other people. It is similar to how people tend to wake up to digital materials of what is going on with real-life friends.

### 5.1.5 Level 1: Phishing

#### Design Rationale

The first topic we selected is phishing since it is topical and common misconception. The interviews conducted prior to the research revealed that there was a misconception regarding the very term, which was understandable when it comes to the basic education. The visual representation of Level 1 is shown in Figure 5,6.

#### Gameplay Breakdown

- **Dialogue with Ahnaf:** The interview displays a scam with a bogus lottery email that replicated local occurrences such as Bkash scams.
- **Teacher Intervention:** they are informed about concepts of phishing by the teacher specialised in NPC.
- **Handout/Notes System:**Notes are saved online so that one can go through them later.
- **Tablet Mini-Game:** To measure the comprehension, the students will select which email is fake or real.

#### Star System:

- Properly classified stars have been assigned.
- Bad classification → feedback messages (Why am I not getting stars?).
- Fast scoring: Speed-based scoring promotes fast responses that are correct.

### 5.1.6 Level 2: Weak Passwords

#### Design Rationale

Once people have heard about phishing, they move on to how it can be avoided. According to the interviews, it happens that many people use weak passwords, you know, like names or birthdays. That is why it is a very significant item to discuss next. The visual representation of Level 2 is shown in Figure 7, 8.

#### Gameplay Breakdown

- **Attempted Login:**Player tries to log-in with a weak password (e.g., `playername123`).
- **NPC Guidance:** Sam describes the rules of powerful passwords, brute force attacks, and proposes two-factor authentication (2FA).

#### Educational Mechanics:

- Players need to make a good password to continue
- Stars are founded on time efficiency and accuracy.

### 5.1.7 Level 3: Free Wi-Fi Risks

#### Design Rationale

Sensitive activities are also usually performed on a Public Wi-Fi without any knowledge of the possible threat such as man-in-the-middle attacks. This stage educates on safe browsing habits and response to breaches. The visual representation of Level 3 is shown in Figure 9,10.

#### Gameplay Breakdown

- Player connects to freepublicwifi to have access to school portal.
- Receives an email later that passwords have to be changed, which indicates security breach.
- Brother NPC informs about the danger and provides the steps to recover, log out, clear cookies, reset a password.

#### Educational Mechanics:

- Simulated post-breach recovery is achieved by interactive tasks.
- Stars- Stars are rewards given upon successful execution of safety measures.

### 5.1.8 Level 4: Malware and Ransomware

#### Design Rationale

This tier deals with the threat of downloading unverified software which is normally posing as free games or applications. The visual representation of Level 4 is shown in Figure 11,12.

#### Gameplay Breakdown

- The player downloads the skins of free games via a counterfeit site(`dungenhunter.com`).
- Earns a ransom mail and files are locked.
- Sam defines ransomware and shows how antivirus can be recovered.

#### Educational Mechanics:

- Virtual learning via simulated files loss.
- The recovery activities help to strengthen prevention and countermeasures.

### 5.1.9 Level 5: Scam Awareness (Mobile and Social Media)

#### Design Rationale

The topmost layer combines social scams such as Bkash scam and allegations of charity, which involves the social aspect of cybersecurity. The visual representation of Level 5 is shown in Figure 13,14.

**Gameplay Breakdown**

- NPC Rimi talks about how fraudulent donation is created and learns how to be more vigilant.
- The player gets a bogus Bkash call where a request is sent concerning an OTP and a loss ensues in case the player enters into it.
- Scam detection and prevention are supported by Brother NPC and a subsequent school seminar.

**Educational Mechanics:**

- both social media and phone-based scams.
- Strengthening of safe behaviors by use of narratives and repetitions.

### 5.1.10 Learning Outcomes

At the conclusion of the game, as shown in Figure 15, players have learned to:

- Recognise phishing emails.
- Use and ensure effective passwords.
- Know risks and steps of recovering public Wi-Fi.
- Unsafe or pirated software should not be downloaded.
- Recognize and avoid scams in the financial or social media.

The role-play, mentorship, and gamified feedback combined will make sure that the learning process is both experiential and corrective and will be remembered by everyone involved.

## 5.2 Game Pilot Testing

There were seven participants in this pilot study, four male, and three female. The key idea was to gather a number of qualitative data points regarding the experience of playing the game, design, and general functionality of the game. The meeting consisted of the members giving the open-minded feedback and suggestions on how the situation can be changed. The information obtained provided insight into multiple problems that kept on reoccurring hence establishing the major weaknesses of the game. Some of the respondents were complaining of the lack of fluidity in movement and transitions in the game: The game does not have fluidity of movement and transitions in places; the transition is not fluid enough. The game, better sound effects, and would be interesting were what one of the other participants said, and that is why it is important to 59 immersive audio design. Additionally, players demonstrated that they experience challenges in learning how to play the game very first as one of the players wrote that The instructions are not very clear; we should have a short tutorial. The research findings were conclusive that the game design

needed significant modifications in three change areas, that is, visual continuity, auditory fidelity and instructional precision. Receiving such judging statements, the development department considered the feedback and made the series of technical corrections. In particular, the sound department was also expanded by voice-overs, which were narrated and increased sound effects, which made the gaming process more immersive and engaging. It was also done in order to make transitions in the game easier and have a more organized system of tutorial that would orient the new players. The net impact of all these gains was to bring more or less substantial gains in efficiency and accessibility and user experience improvements in subsequent assessing tests.

# Chapter 6

# Evaluation: Comparative Controlled Study

## 6.1 Control Study Design

The control study was designed to evaluate the effectiveness of Game-based learning over the traditional approach in terms of enhancing cybersecurity awareness. This study had a controlled experiment following an ethically approved methodology to ensure the fairness, reliability, and validity of the findings. What comes next is an in-depth discussion of the study design process.

### 6.1.1 Primary Objectives

The main objective of this study was to:

- Perform a side-by-side analysis between the gamified and traditional methods.
- Measure the knowledge improvement of the participants across five key cybersecurity topics.
- Determine variations in learning outcomes across demographic groups (urban and rural) and evaluate whether gamified learning fosters higher engagement and retention.

### 6.1.2 Participant Demographics

A total of (n=96) students of age group (10-16 years) were recruited from diverse backgrounds using several sampling methods like voluntary response and convenience sampling methods were used to collect participants in the institutes, and snowball sampling methods were used to pick participants outside institutions. This demographic was selected as adolescents represent a highly active group of internet users who often lack formal cybersecurity training. However, the whole sample size was systematically divided into two experimental groups: the Game-based method group (n=48) and the Traditional method group (n=48). To ensure a balanced and comparable sample, the study maintained an even distribution across key demographic factors. In terms of geographical distribution, exactly half of the participants (50.00%, n=48) were from urban environments, and the other half (50.00%,

n=48) were from rural environments. This one-to-one ratio between urban and rural was maintained within both of the experimental groups. Likewise, there was an equal distribution across the sample size, which was also maintained to balance within each group of the training procedure. Table 6.1 below represents the detailed demographic sample-

| **Group** | **Urban** | **Rural** | **Male** | **Female** | **Total** |
|---|---|---|---|---|---|
| Game-Based | 24 | 24 | 24 | 24 | 48 |
| Traditional | 24 | 24 | 24 | 24 | 48 |
| **Overall (n=96)** | **48** | **48** | **48** | **48** | **96** |

Table 6.1: Participant Demographics Distribution (N=96)

### 6.1.3 Data Collection Process

The data was collected following a two-phase process to measure the knowledge improvement:

- **Pre-Test**: Measured participants' baseline cybersecurity knowledge across five key topics.
- **Post-Test**: Measured immediate improvement in knowledge and applied understanding following the intervention.

This design is consistent with the best practices in the educational context of cybersecurity [44] [43].

### 6.1.4 Assessment Format

The pre- and post-tests were taken using a short quiz format with a numerical point system.

- **Duration**: 15 minutes each.
- **Mode**: Carried out in person in both regions.
- **Language**: The questions were presented both in Bengali and English for the convenience of the participants.

### 6.1.5 Question Development

The scenario-based questions were used to assess both factual and applied learning outcomes. The test consisted of two types of questions:

- **Multiple-Choice Questions (MCQs)**: Consists of 10 factual questions (1 point each) assessing detection-based knowledge (e.g., "Which of these is the strongest password?").

- **Descriptive Scenario Questions**: 5 questions (2 points each) with applied reasoning, problem analysis and response to real-world scenarios (e.g., "If you receive a message asking for your Bkash PIN, how should you respond?").

The following diagram, Fig 6.1, demonstrates the detailed question development with threat-based distribution.

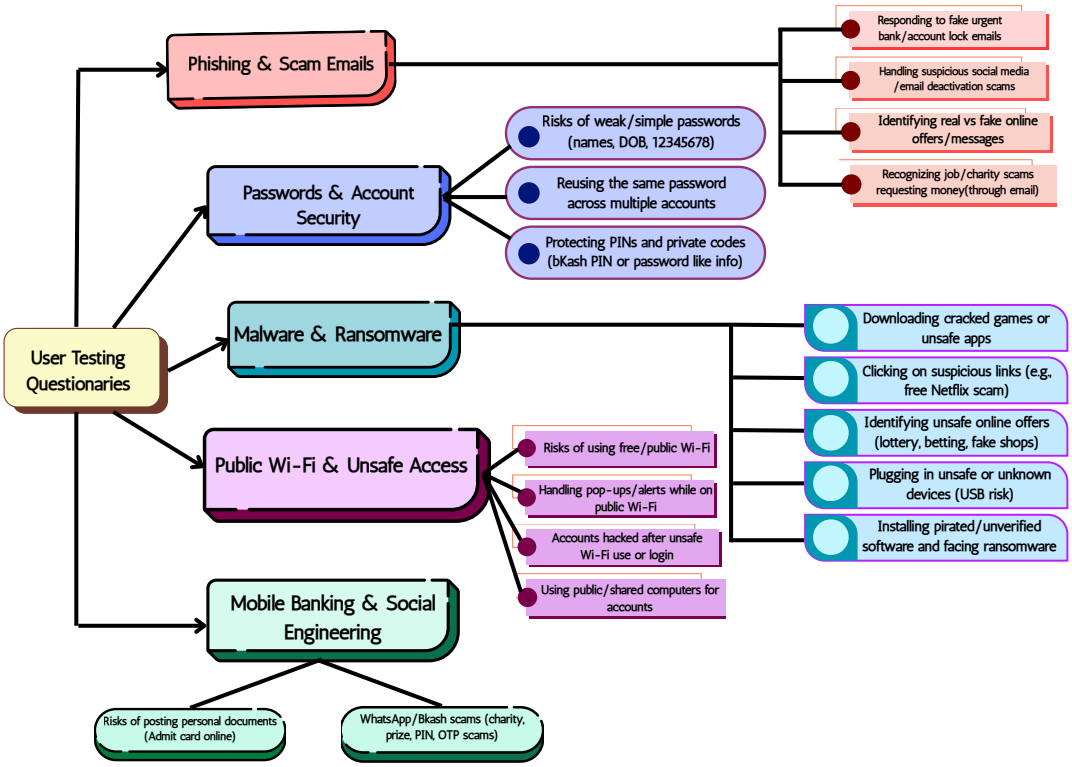



Figure 6.1: Questionnaire Diagram

### 6.1.6 Relevance with the Official Curriculum

Following the semi-structured interviews with older and younger respondents, the findings suggested that younger students were more attracted to our game-based method. In connection with this discovery, we chose the younger audience as the target group and developed special solutions and solutions that consider their needs in learning. To ensure the relevance and accuracy of our intervention, we compared the questions and instructional content employed in our assessments with the contents of the National Curriculum and Textbook Board (NCTB) ICT textbook and realized that these were indeed similar. But in the official curriculum, there are certain cyberthreats that are not included in the curriculum, but our target group is much more vulnerable to them. So, our questions and instructional content were from inside and outside textbook topics. As a result, our gamified platform offers in hand experience in learning the concepts that are included in the NCTB textbook, also outside the curriculum, but important for this target group to learn and be aware of. The main goal was to teach students about basic cybersecurity by introducing the familiar concepts covered in the textbook as well as outside the textbook in an interactive and more engaging manner. In the context of the interview, most of

the students expressed rare interaction with textbooks, referring to the problem of comprehensibility, because they found the texts too heavy with content and tedious. We should always keep in mind the security of our devices [11].

### 6.1.7 Group Distribution

Participants were divided equally into two groups, maintaining parity across demographic and baseline factors:

**Group A (Traditional Method)**

Half members of the sample size (N=48) received instruction through traditional face-to-face (in-class) methods, presentation slides, and instructor-led demonstrations concerning all five cybersecurity topics. The sessions focused on hands-on explanation, visuals and brief conversation to help develop an understanding of key concepts like phishing, weak passwords, malware and online fraud. This approach was representative of the typical education provided in schools in Bangladesh, and it served as the control condition for the study, thus offering a baseline for the gamified learning approach.

**Group B (Gamified Method)**

Remaining half individuals (N=48) participated in playing our developed platform CyberGuard Chronicles, a localised game-based learning experience that uses interactive and experiential learning to teach the same five topics in a cybersecurity learning game. The game offered realistic cyber threat scenarios that challenged players to make informed choices and deploy their knowledge. The levels containing relatable scenarios kept it interesting, and gamification features like points, stars and so on help drive motivation and competitiveness. The material was created with both English and Bangla language support, local currency references, and culturally appropriate examples for the sake of improved comprehension and relatability. Immediate feedback was given at all times in gameplay, increasing understanding and reinforcing retention.
Both groups covered identical content, allowing direct comparison of pedagogical effectiveness. Visual Distribution can be observed from the flowchart Figure 6.2 below:

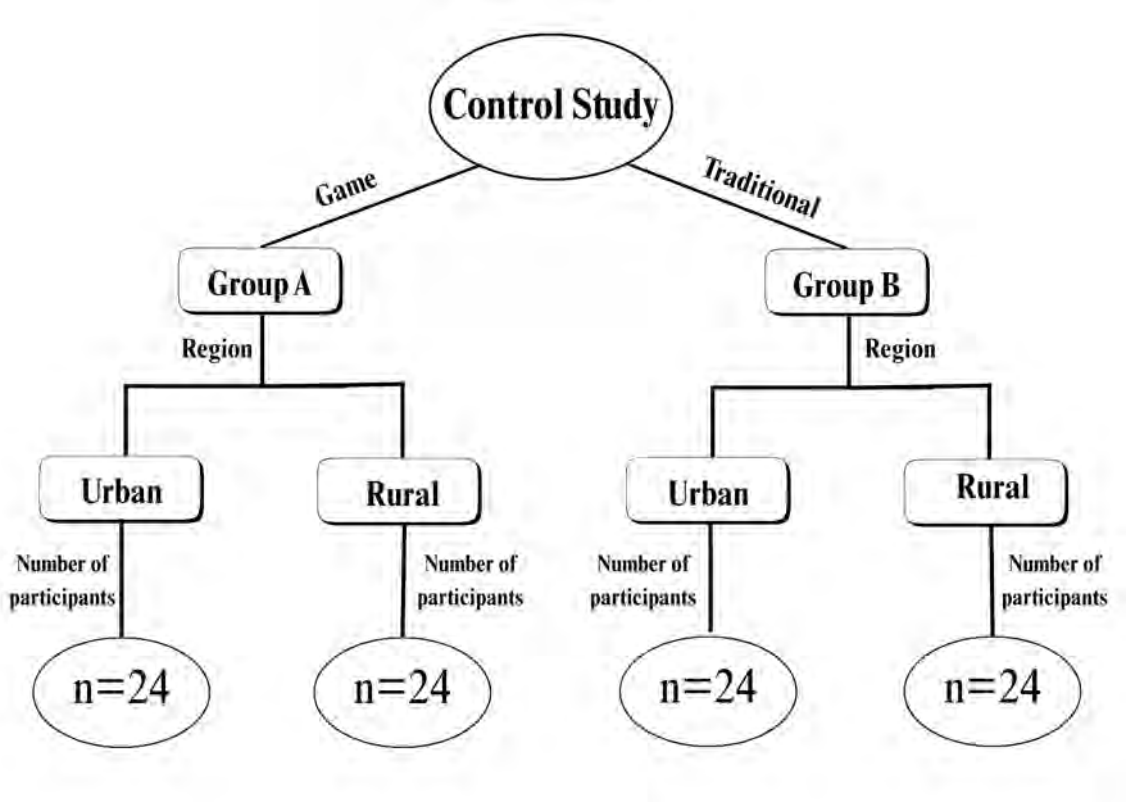



Figure 6.2: Study Flowchart

### 6.1.8 Ethical Considerations

Since the participants were minors, prior informed written consent was taken from their legal guardians and the institutional authorities. In an attempt to preserve privacy, the responses and the metadata were anonymised before any analysis was performed. A case of participation was voluntary, and the students had the right to leave the process at any point and was not charged with any negative impact.

### 6.1.9 Data Management

The test responses were originally recorded on a set of special paper scripts, and then recorded into a safe digital dataset to be analysed, which included item-level scores and associated response information. All the study materials were stored in access-controlled repositories where only the authorised research personnel could access them. As these processes were going on, systematic field notes were kept on a daily basis in every session to record interactions of the participants and any notable behavioural indicators, which supplement the quantitative information.

## 6.2 Findings and Analysis

### 6.2.1 Participants' Response Analysis

The evaluation is based on the proportion of respondents who answered questions assigned during both pre-test and post-test measurements across five central areas of cybersecurity. Improvement rates were computed to gauge the relative efficacy of pedagogic approaches for the induction of cybersecurity awareness.

#### Game-Based Method Results

| Topic | Questions | Pre-Assessment | Post-Assessment | Improvement |
|---|---|---|---|---|
| Phishing | Fake bank emails | 20.8% | 43.8% | 110.0% |
| | Real/fake offers | 8.3% | 41.7% | 400.2% |
| | Social media scams | 12.5% | 37.5% | 200% |
| | Job scams | 14.6% | 33.3% | 128.6% |
| Passwords | Weak passwords | 31.3% | 70.8% | 126.7% |
| | Password reuse | 8.3% | 41.7% | 400.2% |
| | PIN protection | 20.8% | 31.3% | 50.0% |
| Wi-Fi | Free Wi-Fi risks | 2.1% | 66.7% | 3105.3% |
| | Pop-ups | 12.5% | 45.8% | 266.6% |
| | Hacked accounts | 8.3% | 27.1% | 225.1% |
| | Public computers | 4.2% | 20.8% | 399.5% |
| Malware | Cracked games | 27.1% | 52.1% | 92.3% |
| | Suspicious links | 18.8% | 43.8% | 133.3% |
| | Unsafe offers | 12.5% | 35.4% | 183.4% |
| | USB risks | 16.7% | 35.4% | 112.5% |
| | Pirated software | 14.6% | 39.6% | 171.5% |
| Social Eng. | Personal docs | 52.1% | 72.9% | 40.0% |
| | Bkash scams | 35.4% | 75.0% | 111.7% |
| | | | **Average** | **347.6%** |

Table 6.2: Improvement analysis of responses of Group B - Gamification

### Traditional Method Results

| Topic | Questions | Pre-Assessment | Post-Assessment | Improvement |
|---|---|---|---|---|
| Phishing | Fake bank emails | 17.6% | 32.6% | 85.3% |
| | Real/fake offers | 8.3% | 31.3% | 275.2% |
| | Social media scams | 12.5% | 29.2% | 133.4% |
| | Job scams | 12.5% | 25.2% | 101.4% |
| Passwords | Weak passwords | 27.1% | 52.1% | 95.0% |
| | Password reuse | 8.3% | 31.3% | 275.2% |
| | PIN protection | 12.5% | 27.1% | 116.6% |
| Wi-Fi | Free Wi-Fi risks | 14.6% | 50.0% | 242.9% |
| | Pop-ups | 8.3% | 35.4% | 325.2% |
| | Hacked accounts | 6.3% | 25.0% | 300.0% |
| | Public computers | 4.2% | 18.8% | 346.4% |
| Malware | Cracked games | 29.2% | 41.7% | 42.9% |
| | Suspicious links | 16.7% | 35.4% | 112.5% |
| | Unsafe offers | 14.6% | 29.2% | 100.1% |
| | USB risks | 10.4% | 25.0% | 139.9% |
| | Pirated software | 10.4% | 27.1% | 159.9% |
| Social Eng. | Personal docs | 41.7% | 70.8% | 70.0% |
| | Bkash scams | 29.2% | 58.3% | 100.0% |
| | | | **Average** | **167.9%** |

Table 6.3: Improvement analysis of responses from Group A - Traditional

**Comparative Improvement Analysis**

| Topic | Questions | Game Improvement | Trad. Improvement | Difference |
|---|---|---|---|---|
| Phishing | Fake bank emails | 110.0% | 85.3% | 24.7% |
| | Real/fake offers | 400.2% | 275.2% | 125.1% |
| | Social media scams | 200.0% | 133.4% | 66.6% |
| | Job scams | 128.6% | 101.4% | 27.2% |
| Passwords | Weak passwords | 126.7% | 95.0% | 31.7% |
| | Password reuse | 400.2% | 275.2% | 125.1% |
| | PIN protection | 50.0% | 116.6% | -66.6% |
| Wi-Fi | Free Wi-Fi risks | 3105.3% | 242.9% | 2862.4% |
| | Pop-ups | 266.6% | 325.2% | -58.6% |
| | Hacked accounts | 225.1% | 300.0% | -74.9% |
| | Public computers | 399.5% | 346.4% | 53.1% |
| Malware | Cracked games | 92.3% | 42.9% | 49.5% |
| | Suspicious links | 133.3% | 112.5% | 20.9% |
| | Unsafe offers | 183.4% | 100.1% | 83.3% |
| | USB risks | 112.5% | 139.9% | -27.4% |
| | Pirated software | 171.5% | 159.9% | 11.6% |
| Social Eng. | Personal docs | 40.0% | 70.0% | -30.0% |
| | Bkash scams | 111.7% | 100.0% | 11.8% |

Table 6.4: Comparative improvement analysis (Game vs. Traditional)

The given tables (Table 6.2,6.3,6.4) outline the comparative findings of pre-test and post-test outcomes of game-based training and traditional training in basic cybersecurity, comprising phishing, password protection, use of public Wi-Fi, malware, social engineering, and social awareness. The pre-test percentages and the post-test percentages symbolize initial and improved percentages, respectively, as far as awareness of the participants is concerned. The effectiveness of learning depends on the rate of learning improvement as a proportionate shift between the pre-test marks and post-test marks. Overall, the game-based method (347.63%) was reported to have a significantly higher average, compared to the traditional one (167.87%) it which means that the game-based method proves to be more efficient than the traditional approach in terms of increasing cybersecurity awareness levels. Notably, the difference between game-based group participants and traditional group participants was large, and in some aspects, this is improved by more than 3000%. While traditional learning yielded moderate progress, particularly in structured topics like PIN protection, it was less impactful in developing situational awareness. In comparison with Game Improvement (GIm) and Traditional Improvement (TIm), It is sure that the game-based method was superior to traditional training on most issues. These observations suggest that training through simulation is more involving, valuable, and reflects better comprehensiveness of cybersecurity procedures when conducted around socialising communities than training via other methods of pedagogy may show.

### 6.2.2 Statistical Analysis

#### Definition of Terms

- **Traditional Method:** Classroom-based, instructor-led sessions with slides and demonstrations.
- **Gamified Method:** Learning through the game "CyberGuard Chronicles", using interactive and experiential learning.
- **Rural:** Participants from schools in rural areas.
- **Urban:** Participants from schools in urban areas.

#### Game Condition: Paired *t*-test(Pre vs. Post)

We wanted to assess whether the same students exhibit a positive change in test scores after the game-based session by analysing within-student differences using a paired (dependent-samples) t-test at the 5% significance level. A 95% confidence interval (CI) for the mean change is also presented to quantify precision. This is a common method used in cybersecurity and in HCI education research, where pre- and post-intervention measures are taken on the same participants to identify learning gains [43] [55] [54].

#### Hypotheses

Let $d_i = \text{Post}_i - \text{Pre}_i$

- Null hypothesis ($H_0$): $\mu_d \leq 0$ (no improvement or a decrease)
- Alternative hypothesis ($H_1$): $\mu_d > 0$ (there is improvement)

#### T-Test (Paired)

For $i = 1, \ldots, n$:

$$
\begin{aligned}
d_i &= \text{within-student difference} \\
n &= \text{sample size} \\
\bar{d} &= \frac{1}{n}\sum_{i=1}^{n} d_i = \text{mean difference} \\
SD &= \sqrt{\frac{1}{n}\sum_{i=1}^{n}(d_i - \bar{d})^2} = \text{standard deviation} \\
SE_d &= \frac{SD}{\sqrt{n}} = \text{standard error} \\
df &= n - 1 = \text{degrees of freedom}
\end{aligned}
$$

Paired t-test:

$$
t = \frac{\sum d_i}{\sqrt{\frac{n\sum d_i^2 - (\sum d_i)^2}{n-1}}}
$$

**Computations (Game Cohort)**

$$\begin{aligned}
\text{Given } n = 48, \quad \sum d_i = 221.5, \quad \sum d_i^2 = 1323.25 \\
\bar{d} &= 4.61458333 \\
SD &= 2.531166545 \\
df &= 47 \\
SE &= 0.3653424215 \\
t\text{-test (paired)} &= 12.63084454 \\
d_z &= 1.823105374
\end{aligned}$$

**Significance Threshold and Confidence Level**

- Test threshold (one-sided, $\alpha = 0.05$): $t_{0.95,47} \approx 1.677$
- Confidence level for estimation: 95%

**Findings from the Game-Based paired t-Test**

Using within-student differences $d_i = \text{Post}_i - \text{Pre}_i$ for $n = 48$ students in the game condition, we tested $H_0 : \mu_d \leq 0$ (no improvement or a decrease) against $H_1 : \mu_d > 0$ (there is improvement) at one-sided $\alpha = 0.05$ with critical value $t_{0.95,47} \approx 1.677$. From the data ($\sum d_i = 221.5, \sum d_i^2 = 1323.25$), we obtained a mean change $\bar{d} = 4.61458333$ (out of 20), standard deviation $SD = 2.531166545$, and standard error $SE = 0.3653424215$, yielding a paired statistic $t(47) = 12.63084454$ and a very large paired effect size $d_z = 1.823105374$. Because $12.6308 > 1.677$, we reject $H_0$ and conclude that scores improved after the game-based session (one-sided $p < 0.0005$); the one-sided 95% lower confidence bound for the mean gain is:

$$\bar{d} - t_{0.95,47} \approx 4.00$$

This indicates that the true average improvement is at least four points. Overall, the evidence shows a clear, precise, and educationally substantial within-student improvement; an average gain of $\sim 4.61$ points with a conservative lower bound near 4 points, demonstrating a robust positive impact of the game method.

**Traditional Condition: Paired *t*-Test (Pre vs Post)**

We assessed whether the same students exhibit a positive change in test scores after the traditional session by analysing within-student differences using a paired (dependent-samples) t-test at the 5% significance level. A 95% confidence interval (CI) for the mean change is also presented to quantify precision. This method is widely used in classroom-based evaluations and usability studies to detect systematic improvements when the same participants are tested across time [17][13]. In cybersecurity awareness research, paired-sample analyses have been applied to measure how conventional instruction affects learners' ability to recognize and respond to threats, showing its robustness for traditional teaching contexts [42].

**Hypotheses**

Let $d_i = \text{Post}_i - \text{Pre}_i$

- **Null hypothesis** ($H_0$): $\mu_d \leq 0$; it means no improvement or a decrease.
- **Alternative hypothesis** ($H_1$): $\mu_d > 0$; it means there is improvement.

**T-Test (Paired)**

For $i = 1, \ldots, n$:

- $d_i$ = within-student difference
- $n$ = sample size
- $\overline{d} = \frac{1}{n}\sum_{i=1}^{n} d_i$ = mean difference
- $SD = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(d_i - \overline{d})^2}$ = standard deviation
- $SE_{\overline{d}} = \frac{SD}{\sqrt{n}}$ = standard error
- $df = n - 1$ = degrees of freedom

**Paired $t$-test:**

$$t = \frac{\sum d_i}{\sqrt{\frac{n\sum d_i^2 - (\sum d_i)^2}{n-1}}}$$

**Computations (Traditional Cohort)**

Given $n = 48$, $\sum d_i = 135.5$, $\sum d_i^2 = 463.41$

$$\begin{aligned} \overline{d} &= 2.822916667 \\ SD &= 1.312013165 \\ df &= 47 \\ SE &= 0.1893727885 \\ t\text{-test (paired)} &= 14.90666473 \\ d_z &= 2.151591724 \end{aligned}$$

**Significance Threshold and Confidence Level**

- **Test threshold (one-sided, $\alpha = 0.05$):** $t_{0.95,47} \approx 1.677$
- **Confidence level for estimation:** 95%

### Findings From the Traditional-Based paired *t*-test

The post-test scores had a higher average of 2.82 points (out of 20) than pre-test scores across 48 students, with $SD = 1.312013165$ and$SE = 0.1893727885$. The paired test of the within-student difference produced $t(47) = 14.90666473$, $p < 0.0005$, which is greater than the improvement threshold $t_{0.95,47} \approx 1.677$ and shows that there was an improvement in the scores after the old-fashioned session. A one-sided 95% lower confidence bound places the mean gain at $\overline{d} - t_{0.95,47} \approx 2.51$ points, showing the improvement is not only statistically reliable but also sizable in practical terms. The magnitude of the change in question is standardised ($d_z = 2.151591724$), which means that it was a gain and not marginal and isolated. In general, the findings indicate that there was a definite, accurate, and educationally significant within-student change because of the conventional one.

### Game vs. Traditional-Independent *t*-Test on Improvement(post-based)

To find out whether the game-based method results in larger learning improvements than the traditional method, we compared the individual increase in skills between the two independent groups (Game: n = 48; Traditional: n = 48) using a directional (one-sided) Welch independent *t*-test at a = 0.05. Welch's test was selected because it is a non-parametric test that does not assume equality of variance and is commonly used in comparative studies where the variance of the groups may differ. This design is prevalent in the performance evaluation research in HCI and cybersecurity education for analysing performance differences between instructional conditions. When variances or sample sizes are unequal, Welch's test is a better inference test than the standard **t**-test, and it satisfies robust between-group comparison. Its application is consistent with practices followed in the study of usability and awareness in terms of comparative study and research conducted on independent learning intervention[17][38][13][55].

**Hypotheses (one-sided, $\alpha = 0.05$):**

- **Null Hypothesis ($H_0$)**: $\mu_G \leq \mu_T$: This means the gamified solution is not better.
- **Alternative Hypothesis ($H_1$)**: $\mu_G > \mu_T$: This means the gamified solution is better.

## T-test formula:

$$t = \frac{M_1 - M_2}{\sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}}}$$

$$df = \frac{\left(\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}\right)^2}{\frac{(s_1^2/n_1)^2}{n_1 - 1} + \frac{(s_2^2/n_2)^2}{n_2 - 1}}$$

$$SE = \sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}}$$

$$Cohen'sd = \frac{M_1 - M_2}{\sqrt{\frac{(n_1-1)S_1^2+(n_2-1)S_2^2}{n_1+n_2-2}}}$$

Where:

$$M_1, M_2 = \text{Sample mean Improvement}$$
$$S_1^2, S_2^2 = \text{Variance of the two groups}$$
$$n_1, n_2 = \text{Sample size}$$

**Learning Gains(Improvement) by Method (Descriptives)**

| **Metric** | **Game** | **Traditional** |
|---|---|---|
| Sample Size ($n$) | 48 | 48 |
| Mean ($M$) | 4.61 | 2.82 |
| SD ($S$) | 2.53 | 1.31 |
| SE | 0.37 | 0.19 |

Table 6.5: Learning Gains (Improvement) by Instructional Method

**Independent T-test result for Game vs traditional**

| **Metric** | **Value** |
|---|---|
| Mean Difference ($M_1 - M_2$) | 1.791666663 |
| SE | 0.4115059392 |
| $t$-value (Welch) | 4.35392662 |
| df | 71 (70.55545651) |
| $p$ (one-sided, Game > Traditional) | 0.000015 ($p < 0.00005$) |
| $p$ (two-sided, convention) | 0.00003 ($p < 0.0001$) |
| 95% CI for difference (two-sided) | [0.97, 2.61] |
| Cohen's $d$ (Effect Size) | 0.89 |

Table 6.6: Independent T-test results for Game vs Traditional methods

**Findings From the Game vs. Traditional-Independent *t*-Test**

Using individual gain scores (Improvement = Post - Pre), calculated directly from the raw scores of the same 20-point test administered before and after the intervention, the game-based cohort ($n = 48$) achieved a mean improvement of 4.61 points ($SD = 2.53$) on a 20-point test, compared with 2.82 points ($SD = 1.31$) for the traditional cohort ($n = 48$), as shown in Table 6.5, yielding a between-group mean

difference of 1.79 points (≈9% of the total scale). A Welch independent $t$-test was chosen to avoid the equal-variance assumption, which produced $t(\approx 71) = 4.35$ with $\Delta SE = 0.41$ and a one-sided ($p \approx 0.000015$) $p < .00005$ for the prespecified superiority hypothesis (Game > Traditional). For conventional reporting, the two-sided ($p \approx 0.00003$) $p < .0001$, and the two-sided 95% confidence interval for the mean difference was [0.97, 2.61], entirely above zero, indicating a precise advantage for the game method (see Table 6.6). The standardised between-group effect was large (Cohen's $d \approx 0.89$), signifying that the gain attributable to the game-based approach is not only statistically reliable at $\alpha = .05$ but also practically meaningful. In sum, while both methods improved scores, the game-based instruction delivered substantially greater learning gains, and this conclusion is robust to variance heterogeneity and to the more conservative two-sided inferential standard.

**Rural Learning Gains(Improvement) by Method (Descriptives)**

| **Metric** | **Game** | **Traditional** |
|---|---|---|
| Sample Size ($n$) | 24 | 24 |
| Mean ($M$) | 4.78 | 3.02 |
| SD ($S$) | 2.96 | 1.27 |
| SE | 0.60 | 0.26 |

Table 6.7: Learning Gain (Improvement) of Rural by Instructional Method

**Independent T-test result for Rural Game vs Rural Traditional**

| **Metrics** | **Value** |
|---|---|
| Mean Difference ($M_1 - M_2$) | 1.6875 |
| SE | 0.6569 |
| $t$-value (Welch) | 2.5690 |
| df | 31.24 |
| $p$ (one-sided, Game > Traditional) | 0.00510 |
| $p$ (two-sided, convention) | 0.01020 |
| 95% CI for difference (two-sided) | [0.40, 2.97] |
| Cohen's $d$ (Effect Size) | 0.74 |

Table 6.8: Independent t-test result for Rural Game vs Rural Traditional

**Findings From the T-test result for Rural Game vs Rural Traditional:**

Among rural students, the game group improved by $M = 4.71$ (SD = 2.96, $n = 24$) versus $M = 3.02$ (SD = 1.27, $n = 24$) in the traditional group, as shown in the

Table 6.7, giving a mean difference = 1.69 points. Welch's test again favoured the game method, $t(\approx 31.24) = 2.5690$, $\Delta SE = 0.6569$, one-sided $p \approx 0.00510$ (two-sided $p \approx 0.01020$), as reported in the Table 6.8. The 95% CI (two-sided, normal approximation) was [0.40, 2.97], and the effect size was Cohen's $d \approx 0.74$ (medium-to-large). Thus, even with greater score variability in rural settings, the game-based instruction produced reliably larger gains than the traditional method at $\alpha = .05$, amounting to ∼1.7 points (≈ 8.5% of the scale) of additional improvement.

**Urban Learning Gains(Improvement) by Method (Descriptives)**

| **Metric** | **Game** | **Traditional** |
|---|---|---|
| Sample Size ($n$) | 24 | 24 |
| Mean ($M$) | 4.52 | 2.63 |
| SD ($S$) | 2.08 | 1.35 |
| SE | 0.43 | 0.28 |

Table 6.9: Learning Gain (Improvement) of Urban Region By Instructional Method

**Independent T-test result for Urban Game vs Urban Traditional**

| **Metrics** | **Value** |
|---|---|
| Mean Difference ($M_1 - M_2$) | 1.8958 |
| SE | 0.5064 |
| $t$-value (Welch) | 3.7439 |
| df | 39.40 |
| $p$ (one-sided, Game > Traditional) | 0.000091 |
| $p$ (two-sided, convention) | 0.00018 |
| 95% CI for difference (two-sided) | [0.90, 2.89] |
| Cohen's $d$ (Effect Size) | 1.08 |

Table 6.10: Independent t-test Results for Urban Game vs Urban Traditional

**Findings From the Independent T-test result for Urban Game vs Urban Traditional:**

Among urban students, the game group improved by $M = 4.52$ (SD = 2.08, $n = 24$) versus $M = 2.63$ (SD = 1.35, $n = 24$) in the traditional group, as presented in **Table 6.9** yielding a mean difference = 1.90 points on the 20-point scale. The Welch test showed a significant advantage for the game method, $t(\approx 39.40) = 3.7439$, $\Delta SE = 0.5064$, one-sided $p \approx 0.000091$ (two-sided $p \approx 0.00018$), as summarized in **Table 6.10**. The 95% CI for the difference (two-sided, normal approximation) was

[0.90, 2.89], entirely above zero, and the effect size was Cohen's $d \approx 1.08$ (large). In practical terms, urban learners taught via the game-based approach gained nearly 2 points more than their traditional counterparts ($\approx 10\%$ of the scale) with a large, educationally meaningful effect at the $\alpha = .05$ standard.

**Two-Way ANOVA on Improvement**

We tested whether instructional Method (Game vs Traditional) and Demographic (Urban vs Rural) influence students' Improvement, and whether the Method effect depends on Demographic (Method×Demographic interaction). Because the outcome is continuous and predictors are categorical (two Independent Variables: Method and Demographic) with balanced cells (n=24 each; N=96), a 2×2 between-subjects ANOVA is appropriate to assess both main effects and their interaction in a single model while controlling Type-I error. This method is widely used in controlled experiments to examine how multiple independent factors and their interactions are responsible behind differences in learning outcomes, providing stronger explanatory power compared to single-factor tests [38]. In educational and cybersecurity contexts, factorial ANOVA has been applied to evaluate instructional strategies across demographic subgroups, showing its importance for testing both overall effects and subgroup-specific patterns [45][44]. Its ability to reduce inflated error rates while revealing potential interactions makes it a standard choice for multi-factorial designs in HCI and awareness training studies [49].

**Formula:**

$$
\begin{aligned}
SS_{cell} &= \sum_{i,j} n(\overline{y}_{ij} - \overline{y})^2 \\
SS_{method} &= 2\sum_{i} n(\overline{y}_{i} - \overline{y})^2 \\
SS_{demographic} &= 2\sum_{j} n(\overline{y}_{j} - \overline{y})^2 \\
SS_{int} &= SS_{cell} - SS_{method} - SS_{demographic} \\
MS &= \frac{SS}{df} \\
F &= \frac{MS_{Effect}}{MS_{Res}} \\
df_{method} &= 1; \quad df_{demographic} = 1; \quad df_{int} = 1 \\
df_{Res} &= N - 4; \quad \text{where } N = 96
\end{aligned}
$$

Where:

- $n$ = sample size
- $\overline{y}_{ij}$ = cell mean; where $i \in$ method and $j \in$ demographic
- $df$ = degree of freedom
- Effect Size, $\eta^2 = 0.169$

**Demographic and Method Mean of Improvement:**

| Demographic | Method | | Demographic Mean |
|---|---|---|---|
| | Traditional | Game | |
| Rural | 3.0208 | 4.7083 | 3.8646 |
| Urban | 2.6250 | 4.5208 | 3.5792 |
| Method Mean | 2.8229 | 4.6146 | $\overline{y} = 3.7188$ |

Table 6.11: Demographic & Method Mean of Improvement

**ANOVA Table:**

| Source | SS | df | MS | F | P |
|---|---|---|---|---|---|
| Method | 77.0417 | 1 | 77.0417 | 18.666 | <0.001 |
| Demographic | 2.0417 | 1 | 2.0417 | 0.495 | 0.484 |
| MethodxDemographic | 0.2604 | 1 | 0.2604 | 0.063 | 0.802 |
| Residual | 379.7225 | 92 | 4.1274 | | |

Table 6.12: ANOVA Summary for MethodxDemographic

**Findings From the Two-Way Anova:**

The two-way ANOVA on Improvement (see Table 6.12) showed a significant main effect of Method, $F(1, 92) = 18.67$, $p < .001$, partial $\eta^2 = .169$, with Game ($M = 4.61$) outperforming Traditional ($M = 2.82$). There was no main effect of Demographic (Urban vs. Rural), $F(1, 92) = 0.50$, $p = .48$, and no Method $\times$ Demographic interaction, $F(1, 92) = 0.06$, $p = .80$, indicating that the Game advantage is consistent across demographics. To substantiate the pattern at the cell level under mild heteroscedasticity, we conducted post-hoc planned simple-effects (Welch) tests with Holm adjustment: Game > Traditional within Rural ($\Delta = 1.69$, adjusted $p \approx .046$) and within Urban ($\Delta = 1.90$, adjusted $p \approx .004$); within-method Urban–Rural differences were nonsignificant after correction. Overall, the game-based intervention reliably produces larger gains than the traditional approach, regardless of the demographic context.

### 6.2.3 Analysis on Overall Findings

We first started the study by having all of the participants take a short pre-test about cybersecurity to assess the baseline knowledge. Our methodological approach is consistent with Design-Based Research (DBR), an iterative research methodology in which an iterative cycle (pre-test, intervention of the instructional technology, and

post-test) yields a process for polishing both pedagogy and assessment measures. In this study, one entire DBR process was carried out in both rural and urban schools. All students first filled out the pre-test. Each class then got one of two instructional interventions: a game-based lesson with a short lecture on playing roles and narrative rules followed by a facilitated role-play with feedback; or a traditional lecture with a brief lecture presentation and Q&A on secure passwords, phishing, malware, two-factor authentication, and Wi-fi hygiene. Finally, all the participants took the same post-questionnaire. Because each student was given individual pre- and post-test scores, learning gains were calculated by the difference (Post - Pre). The four subject groups (Rural-Traditional, Rural-Game, Urban-Traditional, and Urban-Game), each involving 24 subjects, resulted in a total sample size of 96.

Although both instructional conditions promoted learning, this was done differently. In the Game cohort ($n = 48$), mean improvement was 4.61 points ($SD = 2.53$) on a scale of 20 points, which is statistically highly significant (paired $t(47) = 12.63$, one-sided $p < .0005$) and reflects a large within-subject effect ($d_z \approx 1.82$) (see Table 6.5). The Traditional cohort ($n = 48$) also showed significant improvement with a mean improvement of 2.82 points ($SD = 1.31$) (paired $t(47) = 14.91$, one-sided $p < .0005$, $d_z = 2.15$) (see Table 6.5). Thus, both types of lessons were effective, but the role-play game-based lesson showed higher post-test scores.

Comparing the mean gains of the two groups, the superiority of the Game group ($4.61 - 2.82 = 1.79$ points, about 9% of the maximal score) was significant. A Welch independent-sample $t$-test showed evidence for this difference $t(\approx 71) = 4.35$, one-tailed $p < .00005$; two-tailed 95% confidence interval [0.97, 2.61]; Cohen's $d \approx 0.89$, as summarized in Table 6.6. Pragmatically, the game incorporated design scored almost two points higher than the traditional lesson with regard to scores.

Testing for moderators of the effect of locale, there was virtually no difference between rural and urban students in terms of the effects of the Game condition: Rural students made 4.71 points on average improvements and urban students made 4.52 points, a 0.19 point difference with a Welch $t(\approx 41.32) = 0.25$, $p = .801$. When looking at each setting individually, the instructional benefit remained. The difference in means between Game and Traditional approaches was 1.69 points (Welch $t(\approx 31.24) = 2.57$, one-sided $p \approx .005$; 95% CI, [0.40, 2.97]; $d \approx 0.74$) in favour of using the Game method in Rural schools (see Tables 6.7, 6.8). In Urban schools, the effect was 1.90 points larger (Welch $t(\approx 39.40) = 3.74$, one-sided $p < 0.000091$; 95% CI [0.90, 2.89]; $d \approx 1.08$) (see Tables 6.9, 6.10). A $2 \times 2$ (Method $\times$ Demographic) factorial ANOVA of improvement scores, according to Method and Demographic (urban or rural), yielded a significant main effect of Method (Game > Traditional; $F(1, 92) = 18.67$, $p < .001$, partial $\eta^2 = .169$)), no significant main effect of Demographic ($F(1, 92) = 0.50$, $p = .48$), and no interaction ($F(1, 92) = 0.06$, $p = .80$). In addition, the effectiveness of the game-based approach was similar in both rural and urban situations (see Tables 6.11 and 6.12).

In conclusion, role-play game mechanics-based instructional design is a methodologically substantial and practically conducive way of cybersecurity education. Results are consistent in finding that, compared to traditional lessons, the results in terms

of learning outcomes of this modality are superior on average, show similar benefits across the rural and urban contexts, and demonstrate educationally meaningful Effect Sizes.

## 6.3 Observation Findings: Reading Between the Lines

The user testing sessions uncovered different patterns of emotions and behaviour in the two instruction conditions—Traditional and Game-based learning. Observations were thematically coded according to participants' stated and observed feelings during the sessions.

### 6.3.1 Traditional Condition Observations

#### Anticipation and Initial Reactions

When students heard that they would be in the traditional learning group, many voiced obvious disappointment. Some people were coming to expect them to play the game and, as such, initially didn't find the lecture-style session quite as engaging. However, once the class got started, the facilitators saw curiosity and a willingness to learn from some of the students.

#### Disappointment and Adjustment

During the first half of the session there was mild withdrawal as students had difficulty maintaining attention. Although, the instructor's active approach and practical examples did help to re-engage. Students were increasingly cooperative and on task as the lesson progressed and were flexible and persistent in the face of initial disengagement.

#### Shyness and Social Barriers (Rural Context)

In the rural schools, the students were definitely shy and reluctant to participate. Facilitators were also observed to ask questions openly, leading them to rely on more subtle cues such as facial expressions to assess comprehension. Once trust and familiarity were established, some students were more vocal and engaged. Barriers to interaction based on gender were also commented on; female students were less willing to respond when the class was led by male researchers, but were more at ease with the idea of a female facilitator.

#### Confidence and Cooperation

At the end of the session most students were more confident and more involved. The supportive environment, shared experiences, and guidance from facilitators led to the overcoming of initial reluctance. Despite the disappointing start, the traditional group had a constant cognitive and emotional adjustment throughout the learning process.

### 6.3.2 Game Condition Observations

#### Anticipation and Excitement

In the game condition, enthusiasm was instantaneous. Pupils were thrilled with the prospect of playing a game that would form part of the class and thought that it was a novel and exciting way to learn the lesson, rather than having to learn from textbooks. Younger students (classes 6–8) had higher levels of energy and required short direction to contain their excitement prior to the start of the session.

#### Engagement and Enjoyment

Students engaged and demonstrated a high level of concentration once gameplay had started. Additionally, numerous positive feedback was received, highlighting the fun and engaging way the game made the learning of cybersecurity concepts easier to grasp. One student commented, "I was really able to learn a lot once I put my mind and concentration into it read the conversation. It was fun." They also communicated that they found traditional learning materials boring and uninvolving. On the other hand, when younger targets were asked about the same basic cybersecurity-related topics after listening to some presentations made with the help of our interactive educational game, they said that the experience was much more enjoyable, easier to approach, and comprehend. It was possible to respond to the content and find it more complete and interesting because of the combination of the visual materials, interactive activities, and the learning organization on the basis of the narrative.

#### Anxiety and Performance Pressure

While most students had a positive reaction, a few, especially from classes 9–10, felt slightly anxious and nervous in attempting to do well in the game. The competitive and time-bound aspects induced pressure for some of the participants, but it was not at all a major detriment to the overall learning outcome.

#### Curiosity and Persistence

The gamified environment was highly motivating and created intrinsic motivation. Some students went through the game several times—one student as many as 17 times in the hope that playing again would achieve new levels. The behavioral pattern was portrayed as persistence, self-motivation and an authentic interest in learning the content beyond that which was required.

#### Confidence and Sense of Achievement

While progressing through the levels, the students' confidence grew visibly. The reward system, progress indicators and possibilities for success helped create a sense of accomplishment. Students especially liked the interactive features of the map (for example, flying) that increased both motivation and satisfaction.

Across both instructional conditions, participants experienced a variety of emotions that impacted their level of engagement and learning outcomes. While the traditional method involved active facilitation to take over the initial disengagement and social reluctance, actively, the game-based approach fostered excitement, curiosity and confidence. As a result, the performers had considerably improved in the post-test evaluation, which demonstrated their more advanced, longer, and applied awareness of cybersecurity. Both approaches showed that when learners' emotional states were recognised and managed in an appropriate way, there was meaningful learning taking place despite the emotional journeys that the learners were on. According to these findings, it can be proposed that the educational devices that become gamified can be employed to simplify and make even the complex academic issues more fun, particularly in the case of younger learners who struggle with pursuing the academic curriculum in a textbook format.

# Chapter 7

# Discussion and Future Possibilities

The rapid expansion of information technology and use of the internet in Bangladesh have made awareness of cybersecurity a critical issue. As financial transactions, communications, and information access become increasingly reliant on information technology platforms, citizens at the same time face growing vulnerabilities in cyberspace. How aware and prepared are different segments of society, specifically in comparing youth with older adults, and urban with rural communities, vary profoundly. To factor in on these gaps on cybersecurity awareness, this research will survey critical areas that include password security, fraud, anti-phishing, identity theft, security on accessing networks over Wi-Fi, and anti-malware practice. By mapping awareness gaps and information security practice variation, the work will illuminate those areas which need certain intervention in terms of information security training and information security awareness programs.

## 7.1 Pre-Development Discussion

### 7.1.1 Demographics

The analysis of cybersecurity awareness between age (age groups 10-16 years and 45+ years and geographical locations - urban and rural locations) reveals gaps in awareness and preventive behavior. Younger respondents, and respondents in urban locations in general, have high cybersecurity awareness, through high technology access, educational background, and use of technology, respectively. On the other hand, older respondents and rural groups have low cybersecurity awareness, most evidently through less access to technological technology, no access to information, and less use of cybersecurity training, respectively. According to statistics, urban respondents use additional security controls, but rural respondents use traditional and basic security, and in most cases, with less cybersecurity attack protection.

### 7.1.2 Password Security

The security of passwords continues to present a persistent problem, with significant variation according to age and geographical location. According to the interview analysis, 85% of respondents between 10 and 16 years have password security awareness, yet awareness fails to discourage most from choosing readily discernible information, including names and numbers, for passwords, and therefore heightens

susceptibility to cyberattack. By contrast, adults over 45 years of age have a mere 40% awareness of password security, and a considerable portion practice password reuse between many of their accounts and have no additional security options, such as two-factor authentication (2FA). Urban respondents have a high preference for strong passwords and use 2FA, but rural respondents often miss password updates and rely on simple, guessable passwords. Above all, our analysis shows that 99% of the respondents are not aware of brute force attacks and SQL injection vulnerabilities that are prominent under this kind of security concern. Overall, the trends indicate a severe necessity for password protection training, namely that of older people and inhabitants of rural communities, in a bid to overcome vulnerabilities due to the lack of passwords and authentication methods.

### 7.1.3 Online Scam Awareness

There are several demographic groups in which online scams have been found, but the level of awareness of these scams can be stated as high or low. Among the young participants, approximately 70% are knowledgeable of online scams, and most of them can attribute it to constant utilization of online transactions, online games, and online social networks. Based on our analysis, the 9-10 grade student population is affected by the incidents of online game scams the most. Contrarily, 40% of elderly people, and individuals above 45 years old, are aware, and a majority of them succumb to financial fraud, phone scams, and social schemes scams. Concisely, Social media has been one of the major targets of hackers who seek to obtain personal details on unsuspecting users. The levels of awareness among urban and rural citizens have been 75 and 65 in geographical gaps, respectively, and the difference in their awareness can be attributed to limited access to training on cybersecurity and the skills of technological banks. These statistics reveal a very powerful urge that requires active cybersecurity awareness campaigns, especially to seniors and the rural population, as a successful means to counter financial fraud and scams in the internet space.

### 7.1.4 Phishing and Identity Theft

The level of phishing awareness is pathetically low, especially among elderly people and the rural population. The results demonstrate that merely 40% of the respondents in the young group and 20% of the old age groups are in a position to recognize phishing, indicating that the age groups are heavily trained and informed about cybersecurity. The majority of the participants fail to tell the difference between authentic and fake messages and, hence, are vulnerable to credential hijack and financial fraud. One of our participants said that his accounts got hacked by clicking on a meme, where the attackers got access to the cookies of peoples accounts when the user clicked on the meme photo using a link. In addition, hackers can go beyond just gathering personal information through memes. They can use that intel for more sophisticated social engineering tactics. Urbanites have a high level of awareness (50%) compared to rural communities (30%), which can be attributed to a high level of exposure to security training in companies, institutional programs, and web awareness programs. In a similar manner, awareness about identity theft is moderately high, with youth participants (60%) having a high level of aware-

ness compared to older adults (50%). Despite awareness, most participants have no hands-on expertise in preventing identity theft, including tracking their electronic trails or protecting information in social networks.

### 7.1.5 Wi-Fi Security and Cookie Tracking

The comprehension of security for Wi-Fi varies between age groups, with 50% of youth and 30% of seniors acknowledging danger in case of unsecured networks. There is a significant portion of respondents who continue to use public networks with no use of virtual private networks (VPNs) and proper security settings, putting them at a potential cybersecurity risk. 60% of urban respondents have high awareness and practice proper precaution, but rural respondents, at 40%, overestimate awareness in most cases, a consequence of poor cybersecurity awareness and use of shared network infrastructure. On a contrasting note, awareness regarding cookie tracking is a cause for concern, with only 25% of youth respondents and 5% of seniors reporting awareness about its impact on privacy. What is striking about such an observation is that an immediate training in privacy awareness is a necessity, with many respondents inadvertently allowing information collection.

### 7.1.6 Virus and Malware Protection

The level of awareness about virus and malware danger is remarkably high amongst persons in the youth age group (60%) compared with persons in older age groups (30%), underlining age group discrepancies in technological and cybersecurity awareness. Respondents living in urban settings (70%) exhibit high awareness with regard to antivirus software and safe web browsing behaviour; nevertheless, rural respondents (45%) often lack access to proper cybersecurity tools and updates and become an easy target for malware. Most importantly, respondents with a past encounter with malware exhibit heightened protective behaviour, suggesting that actual experiences with cybersecurity danger enhance hands-on awareness and develop safer behaviour.

### 7.1.7 Views on proposed Solution

The analysis of information collected through an extensive in-person interview in Bangladesh, with a variety of subjects, reveals that the target group—children between 10 and 12 and adolescents between 13 and 16 years of age—has exhibited a significant level of interest in proposed intervention, whereas 68.57% of the older adults(45+) rejected the proposed solution. As per our interview analysis and interview data scraped from the report, and as we've seen a massive interest in playing the game in adolescents they've provided a valuable insight saying they'll play the game because they can educate their other peers while being unduly involved with the game mechanics to be educated. Unlike in previous studies, with a strong bias towards traditional cybersecurity awareness programs, our approach incorporates technological factors in conjunction with a gamification feature for increased learning for the targeted age group. As gaming is a strong attraction for youth in Bangladesh, an interactive platform organized in such a format proves to be

an effective tool for dealing with cybersecurity-related concerns. Participants have exhibited a willingness to use the intervention with a gamified format, with its potential for providing a challenging and effective educational environment in terms of cybersecurity.

The comprehensive report identifies a strong lack of cybersecurity awareness in most demographic segments. Moreover, In the case of taking preventive measures, most of the participants lack proper knowledge of it. Our analysis reveals that the majority of the participants rely on peers or friends rather than official channels whenever they need help for cybersecurity-related help. It also reveals that very few participants think that there is insufficient support from the cybersecurity support system in Bangladesh. The younger respondents and urban respondents in general exhibit a high level of awareness and best security practices, but older persons and rural communities exhibit low cybersecurity awareness, and therefore, are exposed to a high level of digital vulnerability. Areas of concern that require immediate intervention include awareness of social engineering via phishing, the use of password security, and awareness about protecting one's privacy in terms of cookie tracking. Interview Results state that Plenty of account owners whose accounts got hacked fail to understand the recovery procedures needed to get their accounts back. Overcoming such weaknesses through specific cybersecurity awareness programs, digital competency development programs, and training in secure web behaviour will become important for enhancing cybersecurity preparedness in all segments of Bangladesh.

## 7.2 Post-Development Discussion

This study used a clear sequence: we measured what students knew before teaching (pre-test), taught them using a traditional lesson and an RPG (gamified) lesson, and then measured what they learned after teaching (post-test). Both methods were effective, but the role-play(RPG) approach yielded greater overall gains in both locations. In numbers, as shown in Table 6.11, the average improvement in the RPG group was about 4.6, compared with 2.8 in the traditional group. This difference was statistically strong and large enough to matter in real classrooms. The advantage of the RPG approach did not depend on location (no urban–rural interaction), which means the effect is stable across settings. The results show that the RPG approach works very well in both settings. In rural schools, the role-play acted like a bridge. First, we explained the basics of cybersecurity and showed how the role assignments, prompts, and turn-taking work. After that short start, students learned through simple, realistic scenarios inside the role-play. They moved from almost no knowledge to being able to explain and apply ideas such as strong passwords, safer browsing, and basic Wi-Fi safety. The gamified method also assisted students in rectifying misunderstandings and delving into urban schools. They trained themselves to observe the red flags, not to risk downloading, and to know how social engineering works. The students would also have been more receptive to regular lectures, since the lesson is interactive and incorporates the use of clear scenarios with feedback, and students remained focused on remembering. Although the rural and urban students began on different levels, the amount that they learnt during the RPG lesson was roughly similar. This is significant to planning. It implies that the same gamified lesson can be applied in all places. Just one little step with an introduction

of the main words and demonstration of the end feature of role-play controls/flow onboarding in rural schools is sufficient, and the rest of the lesson is the same. The information gives insight into the content focus as well. Basic password rules, device safety, and Wi-Fi were mentioned more by rural students than by urban students, as well as malware, basic passwords, and Wi-Fi, but as a result of the game, phishing, link checks, and avoiding broken apps were discussed more by urban students. This implies a slight modification: provide the rural students with a few more examples on phishing, and the urban students with a few more exercises on how to download safely and on complicated fraud schemes. The gamification strategy requires students to experience decision-making under real conditions, i.e., checking sender details, paying attention to URLs, and declining unsafe attachments, as opposed to reading the rules. This practice is more easily remembered and implemented in the future. Students did not simply repeat the definition, but were practising safer choices in the game and were able to justify the importance of such choices. This explains why we found statistically significant, large, and clear increases in both rural and urban groups with no significant difference between them.

## 7.3 Limitation & Future Work

### 7.3.1 Limitation:

While this study provides valuable insights into the effectiveness of gamified learning for cybersecurity awareness among Bangladeshi adolescents, there are certain limitations that should be acknowledged.

- Though the thesis had a decent sample size of 96 participants, a larger sample size would lead to more unbiased results and generalizable conclusions.
- The control study duration was relatively short. A longer observation period would lead to the difference between what participants know and apply. The attitude–behaviour gap in the participants would have provided more transparent, genuine data.
- The evaluations were conducted in a controlled environment using scenario-based tasks. Participants may overstate their awareness and underreport risky behaviours. Self-reported experiences may have response bias.
- A technical limitation can occur as only the Android version was deployed in the testing environment, which may cause limited accessibility for users on other platforms, such as iOS or desktop systems.

### 7.3.2 Future Work:

To make this research more impactful and vast, certain future implementations can be done, such as:

- Further policy implications can be emphasized in the official curriculum of Bangladesh to incorporate gamified technology as a standard approach to learn and creating awareness in basic cybersecurity and online safety practices.

- For dynamic accessibility, multi-platform deployment should be explored. Extending the application to iOS and web-based platforms would allow broader reach and support classroom integration using shared school devices.
- Future versions of CyberGuard Chronicles can incorporate more levels of more complex cybersecurity concepts so that they can be applicable to a vast age group. So that this technology can be implemented in work sectors as well, for an initial security training. Also, adaptive difficulty settings with dynamically complex scenarios based on difficulty can personalize the learning experience.
- A study with a long duration should be conducted to assess knowledge retention and behavioral transfer over time. Future research could include follow-up assessments after several weeks or a month, and could also implement several simulated experiments to observe real-world behavioral patterns and decision-making capabilities.

# Chapter 8

# Conclusion

Gamification has significant potential in assessment and enhancing cybersecurity awareness and learning, particularly, younger people who are into games and highly active online. However, in the context of Bangladesh, despite the expansion of the internet, many users remain unaware of risks while navigating the internet. In particular, phishing, malware, and privacy breaches are key risks for modern information security. When gamification is evaluated in terms of effectiveness, while the lack of formal cybersecurity education is then juxtaposed (along with the pronounced urban/rural divide as a further qualifier), the urgent need for accessible but engaging forms of learning is plain to see. The general state of vulnerability and the near-ultimate importance of novel approaches to education may be highlighted by the addition of a quote from Pete Cashmore, whose comment states,

***"Privacy is dead, and social media holds the smoking gun...."***

To fill this void, the present research has implemented and created an educational solution, CyberGuard Chronicles, which is a game-like learning platform developed using Unity game engine along with the Firebase database to monitor user activity on edge devices like Android/IOS handsets. These platforms are appropriate for the targeted population as there are substantial user bases of edge devices in Bangladesh. Furthermore, the game uses the information given in the form of contextual real-life examples and Bangla language content, and thus increases the game's relatability and accessibility in the gameplay environment. Comparative analysis of the traditional pedagogical approach against the gamified approach demonstrated that the participants in the gamified system showed increased engagement, reduced response times, and improved conceptual knowledge of key cybersecurity concepts. These results confirm gamification as a pedagogical tool that is effective in bridging awareness and behavior gaps in a variety of demographic groups.

Nevertheless, a number of limitations have been recognized. It describes a general context-sensitive framework for increasing cybersecurity awareness in Bangladesh by adopting a gamified learning system. In this thesis, the details are further expanded on the reasoned and situation-aware framework that is designed to increase cybersecurity awareness in Bangladesh through a gamified method of pedagogy. It begins by clarifying the remaining gaps in the awareness of adolescents and older

adults, and the rationale why traditional lecture-based learning is often not effective in maintaining interest.

From the semi-structured interviews, it was indicative that the younger respondents were more receptive to game-based learning, while older adults were more inclined to learn by using the traditional instructional approach. Based on these results, CyberGuard Chronicles is a role-play game (RPG) experience with localised narratives, characters, and scenarios reflecting the common cybersecurity risks in Bangladesh (phishing, passwords, insecure WiFi, malware, and Mobile Money/Social Media scams), translated into the local language Bengali and tailored to popular mobile platforms. This study focused mostly on the immediate results of learning but did not assess long-term retention or change in behavior.

A subsequent comparative evaluation showed that the game-based instructional approach supported more granular engagement and conceptual understanding as compared to conventional pedagogical modalities, as evidenced to be persistent motivation for learners to reengage and consolidate pivotal concepts. The results show that the gamified approach of cybersecurity awareness in Bangladesh is effective for adolescents and older adults who are vulnerable to unequal access and motivation issues. Based on a human-centred design (HCD) process and semi-structured interviews, the study found the continued lack of understanding of phishing, password hygiene, risks of public Wi-Fi usage, malware, and mobile money or social media scams in the local context. These findings informed the development of the RPG-style game CyberGuard Chronicles, which infused localised narratives and culturally relevant personas and contextualised content that is presented in Bangla, and optimized for the most commonly available mobile devices.

The comparative analysis showed that learner engagement and deeper learning for cybersecurity concepts were found to be higher in the gamified learning design compared to traditional pedagogical methods; learners also showed persistence for revisiting central conceptual ideas. Methodologically, the thesis implements a mixed approach of a combination of qualitative investigation and controlled comparative analysis, which allows for empirical evidence for effectiveness as well as a duly defined overall framework for achieving its goals. The primary contributions of this work are: (i) methodological rigor in interview and statistical validation; (ii) a double-demographic perspective usually lacking in previous studies; (iii) locally sensitive design to the threat landscape of Bangladesh, and (iv) Controlled study findings confirm that gamified learning is more effective than traditional instruction. Therefore, the CyberGuard Chronicles can be considered as a relevant intervention in Bangladesh and a replicable model for culturally responsive cybersecurity education.

Moreover, the educational potential of CyberGuard Chronicles could be further developed by introducing increasing difficulty levels, as well as a greater variety of scenarios covered in the game. It was successfully implemented in both rural and urban schools. Given its successful implementation in rural and urban schools, further expansion into more institutions can help build its potential of being an effective model for the delivery of cybersecurity education in developing contexts such as Bangladesh. Although this study included real-life scenarios and cultural

contextualization, future research should focus on longitudinal studies to evaluate sustained learning outcomes and include simulated phishing tests to measure applied knowledge.

# References


[1] S. Tang, M. Hanneghan, and A. El Rhalibi, "Introduction to games-based learning," in *Games-Based Learning Advancements for Multi-Sensory Human Computer Interfaces: Techniques and Effective Practices*, IGI Global, 2009, pp. 1–17. DOI: 10.4018/978-1-60566-360-9.ch001.

[2] K. M. Gerling and M. Masuch, "Exploring the potential of gamification among frail elderly persons," in *Proceedings of the CHI 2011 workshop gamification: using game design elements in non-game contexts*, 2011, pp. 7–12.

[3] N. A. G. Arachchilage and S. Love, "A game design framework for avoiding phishing attacks," *Computers in Human Behavior*, vol. 29, no. 3, pp. 706–714, 2013. DOI: 10.1016/j.chb.2012.12.018.

[4] I. Caponetto, J. Earp, and M. Ott, "Gamification and education: A literature review," *Proceedings of the 8th European Conference on Games-Based Learning - ECGBL 2014*, vol. 1, pp. 50–57, Oct. 2014.

[5] R. Cox, D. Firestone, O. Kubik, *et al.*, "Security empire: Development and evaluation of a digital game to promote cybersecurity education," in *Proceedings of the 4th USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, 2014, pp. 1–10. [Online]. Available: https://www.usenix.org/conference/3gse14/workshop-program/presentation/cox.

[6] C. Adams and M. Makramalla, "Cybersecurity skills training: An attacker-centric gamified approach," *Technology Innovation Management Review*, vol. 5, no. 1, pp. 5–14, 2015. DOI: 10.22215/timreview/861.

[7] S. Zahir, J. Pak, J. Singh, J. Pawlick, and Q. Zhu, "Protection and deception: Discovering game theory and cyber literacy through a novel board game experience," *arXiv preprint arXiv:1505.05570*, 2015.

[8] G. Jin, M. Tu, T.-H. Kim, J. Heffron, and J. White, "Evaluation of game-based learning in cybersecurity education for high school students," *Journal of Education and Learning (EduLearn)*, vol. 12, no. 1, pp. 150–158, 2018. [Online]. Available: https://download.atlantis-press.com/article/25898444.pdf.

[9] P. Lošonczi, "Importance of dealing with cybersecurity challenges and cybercrime in the senior population," *Security Dimensions*, vol. 26, pp. 173–186, 2018. [Online]. Available: https://www.researchgate.net/publication/328848219_Importance_of_Dealing_with_Cybersecurity_Challenges_and_Cybercrime_in_the_Senior_Population.

[10] I. A. Nabi, "Growth analysis of cybersecurity awareness among mass people of bangladesh: A case study," Accessed: [Insert Date Here], M.S. thesis, Daffodil International University, Dhaka, Bangladesh, Aug. 2018. [Online]. Available: %5BInsert%20URL%20here%5D.

[11] National Curriculum and Textbook Board (NCTB), *Information and Communication Technology: Class 9–10 (Secondary Level)*. Dhaka, Bangladesh: National Curriculum and Textbook Board, 2018.

[12] M. T. Oyshi, M. Saifuzzaman, and Z. N. Tumpa, "Gamification in children education: Balloon shooter," in *2018 4th International Conference on Computing Communication and Automation (ICCCA)*, 2018, pp. 1–5. DOI: 10.1109/CCAA.2018.8777534.

[13] S. Ruoti, J. Andersen, T. Monson, D. Zappala, and K. Seamons, "A comparative usability study of key management in secure email," in *Fourteenth symposium on usable privacy and security (SOUPS 2018)*, 2018, pp. 375–394.

[14] N. Ahmed, M. R. Islam, U. Kulsum, M. R. Islam, M. S. Hossain, and M. M. Rahman, "Demographic factors of cybersecurity awareness in bangladesh," in *2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT)*, IEEE, 2019. DOI: 10.1109/ICAEE48663.2019.8975603.

[15] E. Dilipraj, "South asian cyber security environment: An analytical perspective," Centre for Air Power Studies, Tech. Rep., 2019. [Online]. Available: https://www.researchgate.net/publication/333262265_South_Asian_Cyber_Security_Environment_An_Analytical_Perspective.

[16] W. H. Organization, "Guidelines for the health sector response to child maltreatment," World Health Organization, Tech. Rep., 2019. [Online]. Available: https://www.who.int/docs/default-source/documents/child-maltreatment/technical-report-who-guidelines-for-the-health-sector-response-to-child-maltreatment-2.pdf.

[17] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, "A usability study of five {two-factor} authentication methods," in *Fifteenth symposium on usable privacy and security (SOUPS 2019)*, 2019, pp. 357–370.

[18] BRAC Institute of Governance and Development (BIGD), "Digital literacy and access to public services in bangladesh," BRAC Institute of Governance and Development (BIGD), 2020, Accessed: 2025-01-24. [Online]. Available: https://bigd.bracu.ac.bd/study/digital-literacy-and-access-to-public-services-in-bangladesh/.

[19] S. Hart, A. Margheri, F. Paci, and V. Sassone, "Riskio: A serious game for cyber security awareness and education," *Computers & Security*, vol. 95, p. 101 827, 2020.

[20] R. Roepke, V. Drury, U. Meyer, and U. Schroeder, "Exploring and evaluating different game mechanics for anti-phishing learning games," *Computers & Security*, vol. 95, p. 101 848, 2020. DOI: 10.1016/j.cose.2020.101848.

[21] A. N. Saleem, J. Hamari, J. Koivisto, and T. Gokbulut, "Gamification applications in e-learning: A literature review," *Educational Technology and Society*, vol. 23, no. 3, pp. 1–14, 2020. DOI: 10.1007/s10758-020-09487-x.

[22] M. R. Islam, N. Ahmed, M. M. Mia, U. Kulsum, M. R. Islam, and M. S. Hossain, "Cyber security awareness and cyber crime in bangladesh: A statistical modeling approach," *Australian Journal of Engineering and Innovative Technology*, vol. 5, no. 1, pp. 15–25, 2021. DOI: 10.34104/ajeit.023.015025.

[23] A. Jaffray, C. Finn, and J. R. Nurse, "Sherlocked: A detective-themed serious game for cyber security education," in *Human Aspects of Information Security and Assurance: 15th IFIP WG 11.12 International Symposium, HAISA 2021, Virtual Event, July 7–9, 2021, Proceedings 15*, Springer, 2021, pp. 35–45.

[24] C. Y. Jian and A. Kamsin, "Cybersecurity awareness among teenagers using serious games: A study in malaysia," *International Journal of Emerging Technologies in Learning*, vol. 16, no. 1, pp. 67–85, 2021. DOI: 10.2991/ahis.k.210913.061.

[25] J. Koivisto and A. Malik, "Gamification for older adults: A systematic literature review," *The Gerontologist*, vol. 61, no. 7, e360–e372, 2021. DOI: 10.1093/geront/gnaa047.

[26] B. Onduto, R. Ali, and A. Smed, "Gamification of cyber security awareness–a systematic review of games," *Computing, Faculty of Technology*, 2021.

[27] F. Quayyum, D. S. Cruzes, and M. L. Jaccheri, "Cybersecurity awareness for children: A systematic literature review," *International Journal of Child-Computer Interaction*, vol. 30, p. 100 343, 2021. DOI: 10.1016/j.ijcci.2021.100343.

[28] S. A. Qusa and H. M. Tarazi, "A gamification framework for enhancing cybersecurity awareness in high school students," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 5, pp. 4257–4266, 2021. DOI: 10.1109/CCWC51732.2021.9375847.

[29] N. S. Sulaiman, A. Yacob, N. S. Aziz, *et al.*, "A review of cyber security awareness (csa) among the young generation: Issues and countermeasures," in *Proceedings of the International Conference on Emerging Technologies and Intelligent Systems (ICETIS 2021)*, ser. Lecture Notes in Networks and Systems, vol. 322, 2021, pp. 957–967. DOI: 10.1007/978-3-030-85990-9_76.

[30] B. I. Division, "Bangladesh cyber threat landscape 2022," ICT Division, Bangladesh, Tech. Rep., 2022. [Online]. Available: https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/publications/effc311d_5097_46ba_afa4_5f44b60a93e6/Bangladesh%20Cyber%20Threat%20Landscape%202022.pdf.

[31] B. Fatokun, Z. Awang Long, S. Hamid, O. Fatokun, C. I. Eke, and A. Norman, "An intelligent gamification tool to boost young kids cybersecurity knowledge on fb messenger," in *Proceedings of the 16th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, Seoul, Korea, Republic of: IEEE, Jan. 3, 2022. DOI: 10.1109/IMCOM53663.2022.9721733.

[32] A. Mamun, B. Jamaludin, and S. Mostofa, "Cyber security awareness in bangladesh: An overview of challenges and strategies," *Journal of Information Security*, vol. 9, pp. 88–94, 2022.

[33] R. Matovu, J. C. Nwokeji, T. Holmes, and T. Rahman, "Teaching and learning cybersecurity awareness with gamification in smaller universities and colleges," in *2022 IEEE Frontiers in Education Conference (FIE)*, IEEE, 2022, pp. 1–9.

[34] R. Authors, "A study on cyber attacks detection in bangladesh perspective with machine learning," *ResearchGate*, 2023. [Online]. Available: https://www.researchgate.net/publication/369943531_A_Study_on_Cyber_Attacks_Detection_in_Bangladesh_Perspective_with_Machine_Learning.

[35] R. Authors, "The landscape of cyber crime in bangladesh: Challenges, trends, and mitigation strategies," *ResearchGate*, 2023. [Online]. Available: https://www.researchgate.net/publication/376580933_The_Landscape_of_Cyber_Crime_in_Bangladesh_Challenges_Trends_and_Mitigation_Strategies.

[36] S. Loesch, R. Hrastich, J. Herbert, B. Drangstveit, J. Weber, and M. Vanamala, "Secure arcade: A gamified defense against cyber attacks," *arXiv preprint arXiv:2311.16131*, 2023.

[37] F. Manganello, P. Callaghan, G. Città, *et al.*, "Supercyberkids: Enhancing cybersecurity education in k-12 through digital game-based learning," in *International Conference on Higher Education Learning Methodologies and Technologies Online*, Springer, 2023, pp. 323–334.

[38] M. McCall, E. Zeng, F. H. Shezan, *et al.*, "Towards usable security analysis tools for {trigger-action} programming," in *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, 2023, pp. 301–320.

[39] K. Mclaughlin, "A quantitative study of learner choice in cybersecurity training: Do they even want gamification?" Ph.D. dissertation, Colorado Technical University, 2023.

[40] P. Pirates, *Teaching cybersecurity awareness through gamification: A guide for educators*, Accessed: August 11, 2023. [Online]. Available: https://potatopirates.game/blogs/cybersecurity/cybersecurity-awareness.

[41] R. B. Sağlam, V. Miller, and V. N. Franqueira, "A systematic literature review on cyber security education for children," *IEEE Transactions on Education*, vol. 66, no. 3, pp. 274–286, 2023.

[42] A. C. Tally, J. Abbott, A. Bochner, S. Das, and C. Nippert-Eng, "What mid-career professionals think, know, and feel about phishing: Opportunities for university it departments to better empower employees in their anti-phishing decisions," *Proceedings of the ACM on Human-Computer Interaction*, vol. 7, no. CSCW1, pp. 1–27, 2023.

[43] A. C. Tally, J. Abbott, A. M. Bochner, S. Das, and C. Nippert-Eng, "Tips, tricks, and training: Supporting anti-phishing awareness among mid-career office workers based on employees' current practices," in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 2023, pp. 1–13.

[44] F. Abu-Amara, R. A. Hosani, H. A. Tamimi, and B. A. Hamdi, "Spreading cybersecurity awareness via gamification: Zero-day game," *International Journal of Information Technology*, vol. 16, no. 5, pp. 2945–2953, 2024.

[45] S. Khan, M. Iqbal, O. Osho, *et al.*, "Teaching middle schoolers about the privacy threats of tracking and pervasive personalization: A classroom intervention using design-based research," in *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, 2024, pp. 1–26.

[46] I. Krsek, S. Chen, S. Das, J. I. Hong, and L. Dabbish, "C.a.l.y.p.s.o.: Designing gameplay features for improving player's cybersecurity self-efficacy," in *Companion Proceedings of the Annual Symposium on Computer-Human Interaction in Play*, ser. CHI PLAY Companion '24, Tampere, Finland: Association for Computing Machinery, 2024, pp. 371–376, ISBN: 9798400706929. DOI: 10.1145/3665463.3678832. [Online]. Available: https://doi.org/10.1145/3665463.3678832.

[47] Z. Kuang, X. Xiong, G. Wu, F. Wang, J. Zhao, and D. Sun, "A recommendation system for trigger–action programming rules via graph contrastive learning," *Sensors*, vol. 24, no. 18, p. 6151, 2024.

[48] P. Lieutenant Colonel Saifullah Siddiqui SPP, "Cyber security in bangladesh: Existing threats and the way forward," *The South Asian Times*, Feb. 2024, Accessed: 2025-01-28. [Online]. Available: https://www.thesouthasiantimesbd.com/opinion/news/21748.

[49] N. Miner, A. Abdollahi, C. Myers, *et al.*, "Stairway to heaven: A gamified vr journey for breath awareness," in *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, 2024, pp. 1–19.

[50] D. Pramod, "Gamification in cybersecurity education; a state of the art review and research agenda," *Journal of Applied Research in Higher Education*, 2024.

[51] S. J. Sohrawardi, Y. K. Wu, A. Hickerson, and M. Wright, "Dungeons & deepfakes: Using scenario-based role-play to study journalists' behavior towards using ai-based verification tools for video content," in *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, 2024, pp. 1–17.

[52] G. Tempestini, S. Merà, M. P. Palange, A. Bucciarelli, and F. Di Nocera, "Improving the cybersecurity awareness of young adults through a game-based informal learning strategy," *Information*, vol. 15, no. 10, p. 607, 2024.

[53] S. Wolfswinkel, S. Raghoebar, H. Dagevos, E. de Vet, and M. P. Poelman, "How perceptions of meat consumption norms differ across contexts and meat consumer groups," *Appetite*, vol. 195, p. 107 227, 2024.

[54] Y. Huang, M. Grobler, L. S. Ferro, *et al.*, "Systemization of knowledge (sok): Goals, coverage, and evaluation in cybersecurity and privacy games," in *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, 2025, pp. 1–27.

[55] L. Schoni, I. Sluganovic, M. Strohmeier, and V. Zimmermann, "Stop the clock – counteracting bias exploited by attackers through an interactive augmented reality phishing training," in *CHI Conference on Human Factors in Computing Systems*, ACM, 2025, pp. 1–23. DOI: 10.1145/3706598.3714023.

# Appendix A

This appendix presents the semi-structured interview questions designed to assess participants' baseline cybersecurity awareness, perceptions, and behavioural responses. Each thematic section explores specific areas of online security risks and user understanding. The questions were designed to elicit in-depth insights and qualitative data on awareness gaps, behavioural tendencies, and trust mechanisms in online interactions.

## Demographic Questions

The demographic section aimed to gather background information regarding participants' technological exposure, online activities, and gaming familiarity.

- Name, age, gender and profession/student status.
- Do you own any digital devices? What is your most frequently used device (e.g., smartphone, laptop, tablet)?
- How many years have you been using the internet? Which platforms do you use most often (e.g., Facebook, YouTube, general browsing)?
- Could you describe a typical day in your life? What kind of online activities are part of your daily routine?
- Are you familiar with the term "online game"? Have you ever played online games?
- If yes: What types of games do you usually play? Do you prefer any specific genre?
- If no: Would you be open to trying online games? What type of games would interest you the most?

## Bkash Fraud Scenario

### Objective

To understand how individuals perceive and respond to online financial scams, specifically focusing on the mechanisms of trust-building and susceptibility to deception.

### Interview Questions

1. Have you ever heard the term “online scamming” or “social engineering”?
2. If yes:
   2.a. Do you know how to prevent such scams?
   2.b. If yes, how would you prevent them?
3. If no: (Gap identified — participant lacks knowledge about prevention methods.)

### Scenario Description

> Suppose you receive a phone call from someone claiming to be a Bkash agent or customer care representative. They tell you that your account has been blocked or that money has been mistakenly transferred to your account. Shortly after, you receive a text message that appears to support their claim. The caller asks you to share your OTP or send the money back immediately.

### Follow-Up Questions

- Have you ever encountered such a situation?
- If yes: How did you or someone you know respond?
- If no: How would you handle this situation if it happened to you?
- What do you think this type of scam is called?

### Expected Preventive Awareness

- Always verify the identity of callers by contacting official sources directly.
- Avoid sharing sensitive information such as OTPs or passwords over the phone.
- Stay calm and avoid acting under pressure or urgency created by the scammer.
- Verify transactions through official statements before taking any action.
- Educate yourself on mobile banking procedures and online financial safety.

## Online Game Scams

### Objective

To identify awareness levels and behavioral responses toward financial scams embedded in gaming environments.

### Scenario Description

Imagine one of your friends calls you excitedly and tells you about a new game where you can earn instant rewards. The offer sounds too good to be true: "Register with 500 taka and get 1000 taka instantly!" The friend claims to have already earned a large amount and insists that you join as well, describing it as a quick and easy way to make money.

### Interview Questions

1. Have you ever played online games?
2. If yes:
   - 2.a. What types of games do you generally play?
   - 2.b. Have you ever heard about online game scams?
   - 2.c. How did you learn about them, and do you know how to prevent them?
3. If not: (Gap identified — lack of awareness about gaming scams.)
4. Have you or anyone you know experienced an offer similar to the scenario described?
5. How did you or they respond?
6. How likely are you to trust such offers, and why?
7. Do you think such offers are scams? How can they be identified?

### Expected Preventive Awareness

- Be skeptical of unrealistic financial offers or rewards in online games.
- Avoid investing money in unverified or suspicious gaming platforms.
- Research the source and authenticity of the offer before engaging.
- Understand that illegal gaming websites can lead to identity theft and data leaks.

## Fake Charity Scams

### Scenario Description

You come across a Facebook post or message requesting donations for an urgent cause, such as helping a sick person or flood victims. The post includes a mobile payment number or bank account. Later, you discover that the account was fake and unrelated to the claimed cause.

### Interview Questions

1. Have you ever donated online to charity or relief funds?
2. Are you aware of scams involving fake charities?
3. Do you know how to verify the authenticity of such pages or posts?
4. Have you or anyone you know experienced such scams?
5. How would you respond if you found out that the charity was fake?

### Expected Preventive Awareness

- Avoid emotional decision-making triggered by urgent donation requests.
- Always verify donation links and payment details through official channels.
- Avoid clicking on unverified links or sharing personal payment information.
- Promote awareness of verified and trusted charities to prevent misinformation.

## Identity-Based Attacks (Cookie Tracking)

### Scenario Description

> Suppose you install a browser extension promoted by a YouTuber that promises shopping discounts. Soon after, you notice an increase in ads, browser pop-ups, and suspicious activity in your email and social media accounts.

### Interview Questions

1. Do you frequently browse different websites apart from social media?
2. Have you heard of "identity theft" or "cookie tracking"?
3. What do you understand by cookie-based scams?
4. Do you usually click "Accept Cookies" without verifying website authenticity?
5. Have you experienced or heard of similar situations?
6. How would you handle it if such activity occurred on your device?

### Expected Preventive Awareness

- Be cautious when accepting cookies or installing browser extensions.
- Verify the authenticity of websites and plugins before granting permissions.
- Use trusted browsers and clear cookies regularly to reduce tracking risks.

# Phishing Attacks

## Scenario Description

While browsing social media, you receive a message from a familiar contact sharing a link to a video with an attractive caption. The link redirects to a fake login page resembling a legitimate website that collects your credentials.

## Interview Questions

1. Do you know what a phishing attack is? Could you describe it in your own words?
2. Have you or someone you know experienced phishing before? How did you handle it?
3. Do you believe phishing attacks are common in Bangladesh? Why or why not?
4. What advice would you give to someone who falls victim to phishing?

## Expected Preventive Awareness

- Avoid clicking on suspicious links or attachments.
- Verify sender identities before sharing information.
- Use two-factor authentication for added security.
- Never provide passwords or financial information through unofficial sites.

# Weak Password Attacks

## Interview Questions

1. How frequently do you use the internet, and for what purposes?
2. Do you use applications or websites that require login credentials?
3. What do you know about weak passwords?
4. Are you familiar with brute-force or SQL injection attacks?
5. How often do you change your passwords?
6. Do you use two-factor authentication?
7. How would you respond if your account was hacked?
8. What strategies can be used to create strong and secure passwords?

### Expected Preventive Awareness

- Use a combination of letters, numbers, and special characters in passwords.
- Avoid reusing passwords across different platforms.
- Enable two-factor authentication.
- Change passwords regularly and avoid predictable information.

## Wi-Fi Security Issues

### Scenario Description

> Recent reports highlight major data breaches caused by weak Wi-Fi security. Hackers often exploit public Wi-Fi networks or set up fake "evil twin" networks to intercept user data.

### Interview Questions

1. How often do you use Wi-Fi to connect to the internet?
2. Do you connect to public Wi-Fi networks? If yes, why?
3. Are you aware of Wi-Fi-related security risks?
4. What would you do if you discovered unauthorized access to your Wi-Fi?
5. How can individuals and businesses ensure Wi-Fi security?

### Expected Preventive Awareness

- Avoid connecting to unprotected public Wi-Fi.
- Verify network names before connecting.
- Use VPNs when accessing sensitive data.
- Regularly update router passwords and firmware.

## Virus and Malware Attacks

### Scenario Description

> You receive an email containing an image attachment. After opening it, your webcam and microphone activate unexpectedly, and you later discover your account was hacked.

## Interview Questions

1. Do you know what viruses or malware are?
2. Have you or someone you know experienced a malware attack?
3. What do you know about Trojan or RAT (Remote Access Trojan) attacks?
4. How often do you download software from unverified sources?
5. How would you respond if your device showed suspicious behavior?

## Expected Preventive Awareness

- Install and update antivirus software regularly.
- Avoid downloading attachments or software from unknown sources.
- Monitor and limit camera/microphone permissions.
- Use a physical cover for webcams when not in use.

# Appendix B

This appendix presents the multiple-choice questions (MCQs) and scenario-based questions designed to evaluate participants' cybersecurity awareness, including password safety, phishing, scams, and public Wi-Fi risks.

## Multiple Choice Questions (MCQs)

1. Fatema is trying to open a Facebook account for the first time. She set `Kopil123` as her password, which her sister Faima guessed easily. Choose a password for Fatema which will be hard to guess:

    - Kopil@2005
    - F@t3ma123
    - T@ble!97#
    - Bangladesh#1

2. Siam used his date of birth `15012005` as his email password. Is using birthdays as passwords safe?

    - Yes, because numbers look random and hard for computers to break
    - Yes, because passwords made of numbers are harder to crack than words
    - No, because birthdays are long, and long passwords are always insecure
    - No, because personal details like birthdays are the first thing attackers try

3. Nusrat got a login alert: someone knew her Gmail password but couldn't log in because an OTP was sent. Is the password alone enough?

    - Yes, because the password is always the final security step
    - No, because 2FA requires both the password and the second factor
    - Yes, because OTPs only protect banking apps, not emails
    - No, because Gmail blocks logins if the device looks unfamiliar

4. Shafin connected to free Wi-Fi in a café and later noticed suspicious login notifications. Is connecting to free Wi-Fi concerning?

    - No, because free Wi-Fi is safe if it's widely available in public places
    - No, because using "https://" websites protects you completely

- Yes, because attackers can create fake Wi-Fi networks with convincing names
- Yes, because free Wi-Fi is only risky if the network has no password

5. Shorna received a suspicious bank email claiming urgency. Do banks send such emails?
   - No, because phishing emails often mimic real banks to steal credentials
   - Yes, because banks always send urgent emails to verify accounts
   - Yes, because if the email contains the official logo, it must be safe
   - No, because banks never send emails about account issues
6. Hasan downloaded "free cracked games" and faced malware issues. Why is an antivirus needed?
   - Yes, because antivirus mainly improves system speed
   - Yes, because antivirus is only useful to protect against hackers
   - No, because antivirus prevents ads on websites
   - No, because antivirus is designed to detect and remove malware infections
7. Maliha posted her exam admit card online. Is this safe for social media friends verification?
   - No, because sensitive details can be used for scams or identity theft
   - Yes, because she shared it only with friends
   - Yes, because showing an official document is safer than writing personal info
   - No, because the post can be deleted later
8. Rafi received a WhatsApp link for free Netflix. Is it safe to click?
   - Yes, because if it looks professional, it must be safe
   - No, because such links often lead to scams that steal information
   - Yes, because the number is saved in your contacts
   - No, because you're only at risk if you type your password afterwards
9. Rahim received multiple online offers. Are all offers equally safe?
   - Yes, but everything online is potentially a scam
   - Yes, because betting websites are always safe
   - No, because verified HTTPS online shops are generally legitimate
   - No, because prize SMS from unknown numbers are always genuine
10. Tania considered using one password for all accounts. Is it safe?
    - Yes, because one strong password reduces the need to remember multiple passwords

- No, because using unique and strong passwords for each account prevents multiple accounts from being hacked
- Yes, because trusted family members can safely manage your passwords
- No, because using birthdays or personal info makes passwords long and hard to guess

11. Which of these is NOT a cyber scam?
    - Fake BKash prize messages
    - Charity fraud messages
    - Sports betting fraud
    - Using a HTTPS website

# Scenario-Based Questions

1. **Scenario:** Rahim receives a message: *"Congratulations! You've won 1,000 BDT. Send your BKash PIN immediately to claim it."*
   What should Rahim do, and why is sharing the BKash PIN risky?

2. **Scenario:** Sumaiya receives a WhatsApp message: *"Send 500 BDT to help poor children. Your donation will be verified."*
   How should she respond, and how can she verify if the charity is genuine?

3. **Scenario:** Tanvir receives an email from his school: *"Click here to download your exam results immediately!"* with spelling mistakes.
   What is the safest action and why is clicking dangerous?

4. **Scenario:** At a café, Arifa connects to free Wi-Fi. A pop-up appears: *"Your device is infected! Download this app now to clean it."*
   What should she do, and why is downloading unknown apps from public Wi-Fi risky?

5. **Scenario:** Farzana connects to "Free_Internet_4U" Wi-Fi and notices login attempts from unknown locations.
   What steps should she take to secure her accounts, and what habits can protect personal information when using public Wi-Fi?

# Appendix C

This appendix presents the multiple-choice questions (MCQs) and scenario-based questions designed to evaluate participants' cybersecurity awareness, including password safety, phishing, scams, and public Wi-Fi risks.

## Multiple Choice Questions

1. Rafi receives a message: "Your bank account has been locked. Click here to verify immediately." Which action is safest?

   (a) Click the link in the message and follow the verification steps shown.

   (b) Call the phone number printed in the message to confirm the lock.

   (c) Call the bank using the phone number on the back of your card or official website.

   (d) Reply to the message asking the sender who they are and why the account was locked.

2. Siam sets his password as 12345678. A friend guesses it easily. Which password strategy would be safest?

   (a) Construct a long, unique passphrase that mixes uppercase/lowercase letters, digits, and punctuation.

   (b) Switch to a different simple numeric sequence (e.g., 87654321).

   (c) Temporarily use a trusted friend's password then change it later.

   (d) Pick one strong-looking password and reuse it across all accounts.

3. Arifa's phone shows: "Critical update available! Install to secure your device." What should she do?

   (a) Install the update immediately from the popup.

   (b) Verify the update through the official app store or vendor's website before downloading.

   (c) Ignore all update notifications permanently.

   (d) Forward the popup screenshot to friends asking for advice.

4. Farhana connects to "Library_Free_WiFi" and logs into her email. Later, she notices unusual login alerts. What is the safest approach?

   (a) Continue using the Wi-Fi normally.

(b) Share the Wi-Fi password with friends.

(c) Disconnect from the free Wi-Fi immediately and switch to a VPN or secure network.

(d) Install random security apps suggested by pop-ups.

5. Farhan used the same password across many sites. A small online shop's database leaked. Which steps should be taken?

   (a) Change bank and email passwords first.

   (b) Set the same new password on all sites.

   (c) Check each site's recent login/activity logs.

   (d) Install a password manager and generate unique passwords.

6. Maya placed an online order. She then received an invoice from the company's official email address. Which is generally NOT a cyber scam?

   (a) A message saying she won a "lucky draw gift" for shopping once.

   (b) An invoice from the company's official email for her actual order.

   (c) An email claiming her order failed and asking for card details again.

   (d) An "order confirmation" email with a software attachment.

7. Tanvir receives: "Your Instagram account will be deactivated. Log in immediately!" The link leads to a random login page. Correct response?

   (a) Verify the account status via the official website or app.

   (b) Click the link immediately.

   (c) Forward the email to friends asking for advice.

   (d) Reply to the sender asking why the account is being deleted.

8. Shahin downloads a "game hack app" from an unofficial site. Pop-ups appear. What should he have done first?

   (a) Install and share the app with friends.

   (b) Read user reviews, verify developer's identity, then download.

   (c) Scan the downloaded file with antivirus before installing.

   (d) Ignore security warnings.

9. Subarna received a WhatsApp message from an unknown number: "Free Netflix Premium 1 year — click to verify." The link asks for a phone number then an OTP. What should she do?

   (a) Send the OTP.

   (b) Ignore the link, block and report the number.

   (c) Verify the offer only via Netflix's official website or app.

   (d) Reply asking for clarification.

   (e) Never provide personal or banking details if requested later.

10. Nabila logs into email on a library computer. Later, her account sends spam messages. Correct preventive action?

    (a) Avoid using public computers or log out after use.

    (b) Continue using public computers normally.

    (c) Use incognito mode and two-factor authentication.

    (d) Share login details with trusted friends for monitoring.

    (e) Ignore suspicious activity as a random glitch.

## Scenario-Based Questions

1. Rafi receives an email offering a high-paying remote job but asks for a "training fee." How can Rafi determine legitimacy and protect personal/financial info?

2. Ayan notices an alert that someone accessed his cloud storage from another country. What steps should he take immediately, and how could his account have been compromised?

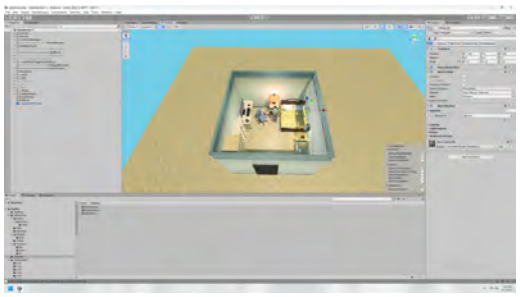
3. At a café, Hasan finds a USB drive labeled "Exam Answers." He plugs it in. Why is this risky, and what measures should Hasan take to avoid malware or data theft?

4. Maliha posts a picture of her exam admit card showing her roll number, DOB, and phone number. What risks does she face, and how can she safely share content on social media?

5. Shahin downloads a "premium Photoshop for free" from a flashy website. His computer slows and pop-ups appear. What went wrong, and how could Shahin verify software safety before downloading in the future?

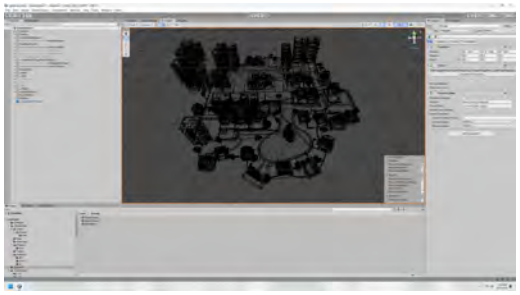
# Appendix D

## Game Environment and Character Design



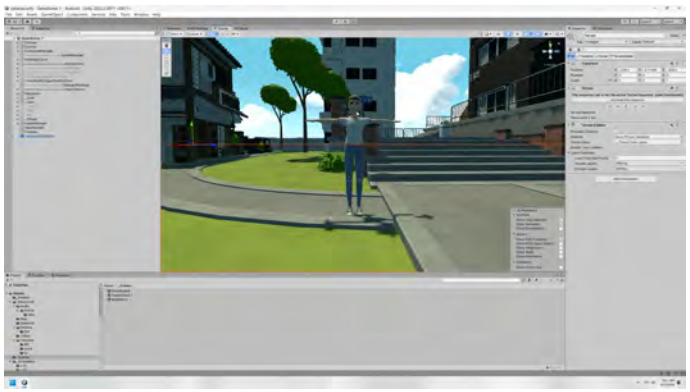
(a) Map of the game room layout.

(b) Overview of the game environment.



(c) Alternative view of the environment.

(d) Alternative view of the environment-2.



(e) character in the environment.

Figure 1: Screenshots from CyberGuard Chronicles showing maps, environment, and character design.

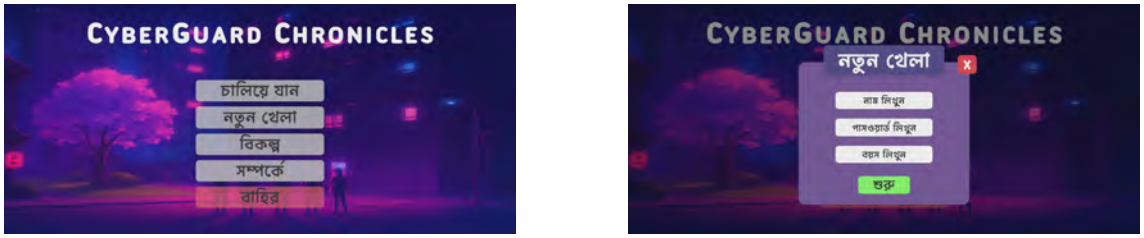
# Player Registration Screens

**English Version:**


(a) Main Menu (b) Player Registration

Figure 2: Player Registration(English)

**Bangla Version:**




(a) Main Menu (b) Player Registration

Figure 3: Player Registration(Bangla)

# Game Interface(GUI)

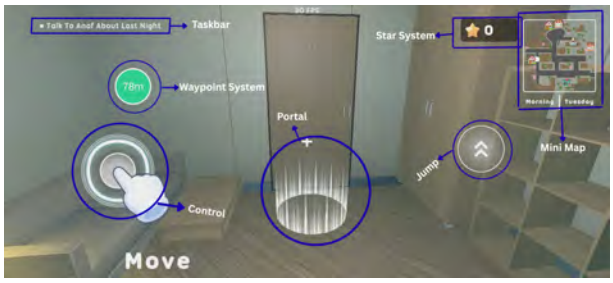


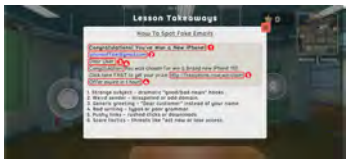

Figure 4: Overview of game interface and control layout

# Level-wise Gameplay Screenshots

## Level 1: Phishing

**English Version:**


(a) Level-1 start interface.



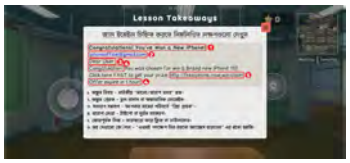

(b) In-game notes (learning outcomes).


(c) Feedback: "Why am I not receiving stars?"

Figure 5: Screenshots from Level 1(English): Phishing- showing the level introduction, in-game notes, and feedback interface.

**Bangla Version:**


(a) Level-1 start interface.




(b) In-game notes (learning outcomes).

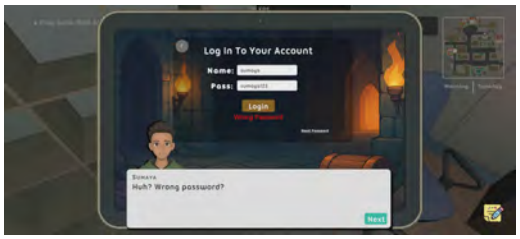

(c) Feedback: "Why am I not receiving stars?"

Figure 6: Screenshots from Level 1(Bangla): Phishing- showing the level introduction, in-game notes, and feedback interface.

## Level 2: Weak Passwords

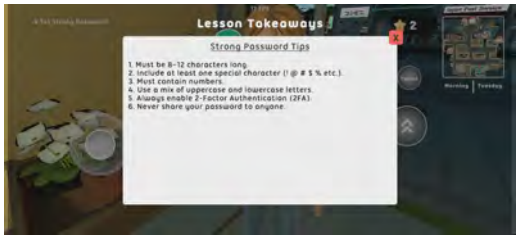
**English Version:**


(a) Level 2 start interface.




(b) Login attempt failed due to weak password.

(c) Sam explaining strong password rules and 2FA.

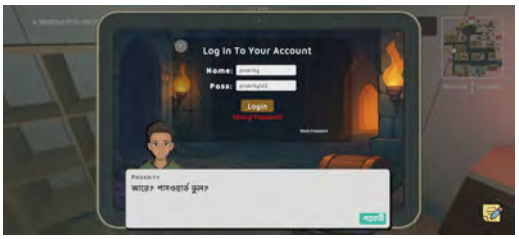



(d) Important note on creating strong passwords.

Figure 7: Gameplay stages in Level 2(English): Weak Passwords.

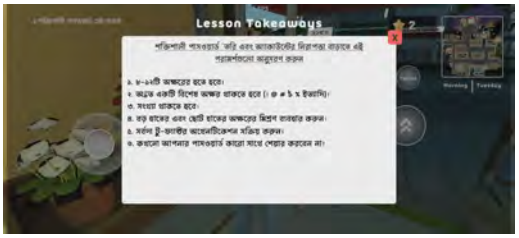
**Bangla Version:**


(a) Level 2 start interface.




(b) Login attempt failed due to weak password.

(a) Sam explaining strong password rules and 2FA.



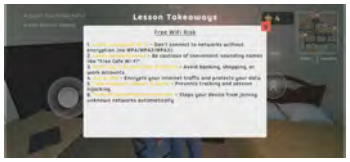

(b) Important note on creating strong passwords.

Figure 8: Gameplay stages in Level 2(Bangla): Weak Passwords.

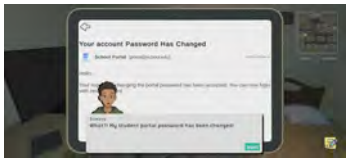
## Level 3: Free Wi-Fi Risks

### English Version:


(a) Level start: connecting to public Wi-Fi.




(b) Important Notes on Connecting to Free-WiFi.

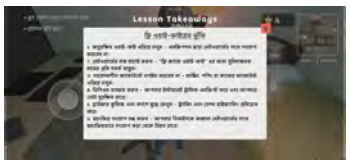



(c) Player experiences the Wi-Fi breach event.

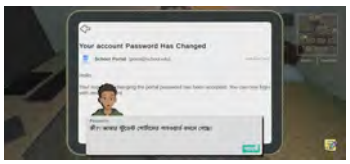
Figure 9: Gameplay sequence of Level 3(English): Free Wi-Fi Risks.

### Bangla Version:

(a) Level start: connecting to public Wi-Fi.




(b) Important Notes on Connecting to Free-WiFi.



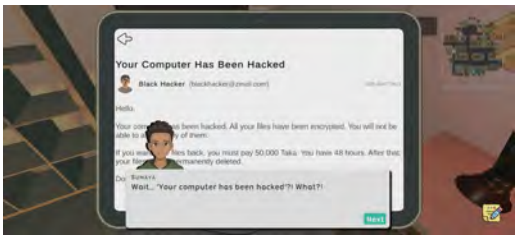

(c) Player experiences the Wi-Fi breach event.

Figure 10: Gameplay sequence of Level 3(Bangla): Free Wi-Fi Risks.

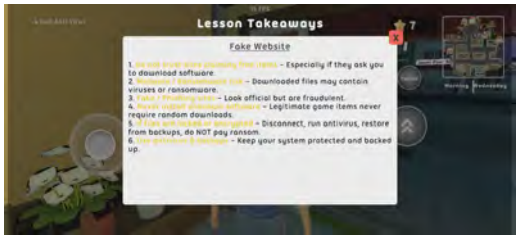
## Level 4: Malware and Ransomware

### English Version:

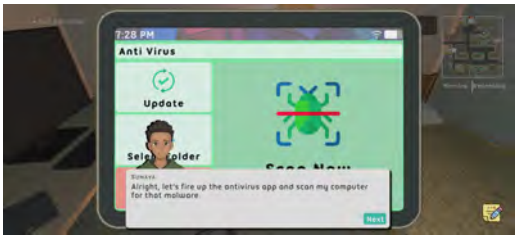

(a) Level start: downloading from an unverified website.




(b) Files locked after the ransomware attack.




(c) Important notes on malware and ransomware.

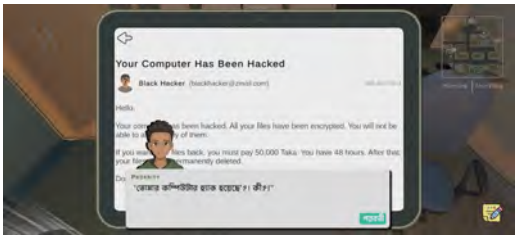



(d) Antivirus scanner demonstrating file recovery.

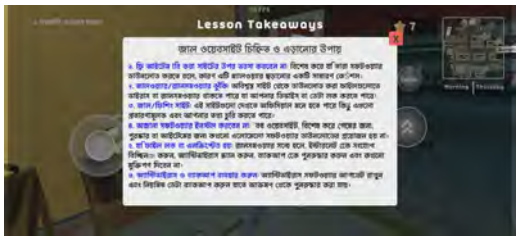
Figure 11: Gameplay sequence of Level 4(English): Malware and Ransomware.

**Bangla Version:**

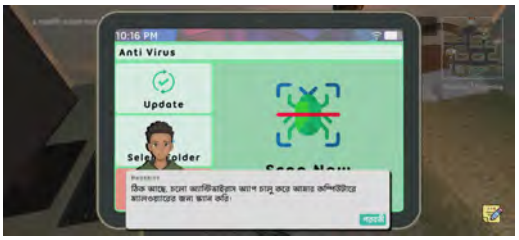

(a) Level start: downloading from an unverified website.




(b) Files locked after the ransomware attack.




(c) Important notes on malware and ransomware.



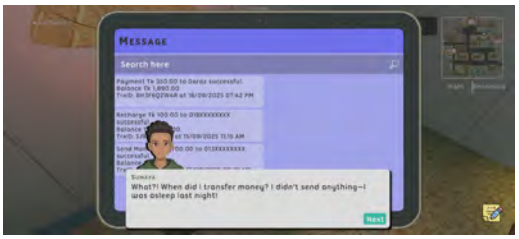

(d) Antivirus scanner demonstrating file recovery.

Figure 12: Gameplay sequence of Level 4(Bangla): Malware and Ransomware.

## Level 5: Scam Awareness (Mobile and Social Media)

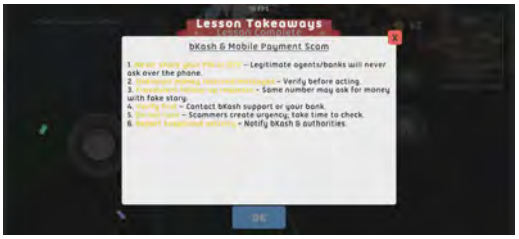
**English Version:**


(a) Level start: introduction to scam scenarios.




(b) Player gives PIN and Bkash account gets compromised.

(c) Brother NPC explains how the scam might have occurred.

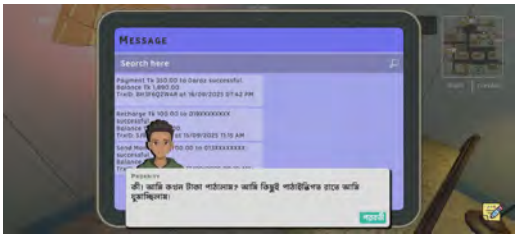



(d) Notes on online scams and safe practices.

Figure 13: Gameplay sequence of Level 5(English): Scam Awareness (Mobile and Social Media).

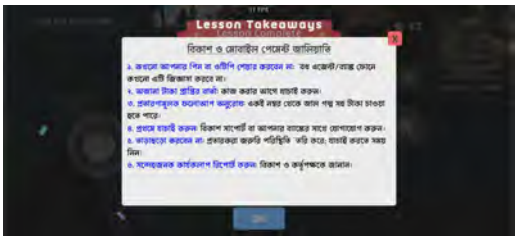
**Bangla Version:**


(a) Level start: introduction to scam scenarios.




(b) Player gives PIN and Bkash account gets compromised.

(c) Brother NPC explains how the scam might have occurred.




(d) Notes on online scams and safe practices.

Figure 14: Gameplay sequence of Level 5(Bangla): Scam Awareness (Mobile and Social Media).

## Overall Learning Outcome

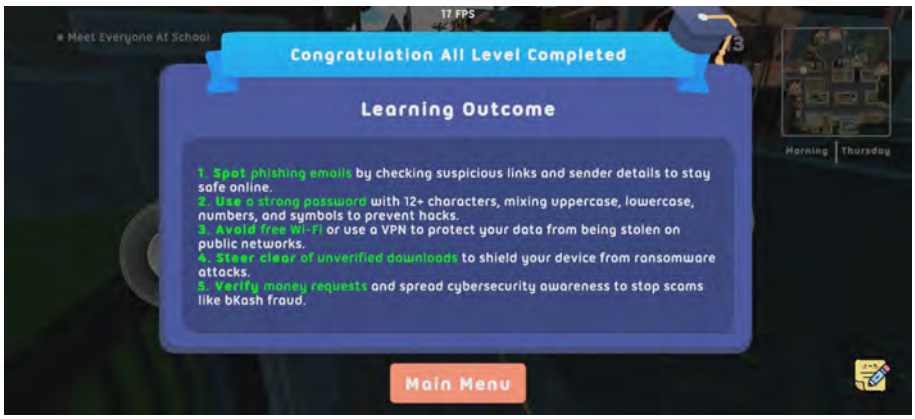



Figure 15: Summary of learning outcomes achieved through gameplay.