The Exiled Prince: A Human-Centered Digital Game for Promoting Cybersecurity Awareness and Engagement among Non-CS University Students in Bangladesh

by

MD. Atiq Mahbub
22141013
Nouruzzaman Niloy
22141004
Mirza MD. Shafi Uddin
21301586

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 and Engineering

Department of Computer Science and Engineering
Brac University
October 2025.

Declaration

It is hereby declared that

1. The thesis submitted is 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:

MD. Atiq Mahbub

22141013

Nouruzzaman Niloy

22141004

Mirza MD. Shafi Uddin

21301586

Approval

The thesis/project titled "The Exiled Prince: A Human-Centered Digital Game for Promoting Cybersecurity Awareness and Engagement among Non-CS University Students in Bangladesh" submitted by

1. MD. Atiq Mahbub (22141013)
2. Nouruzzaman Niloy (22141004)
3. Mirza MD. Shafi Uddin (21301586)

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

Examining Committee:

Supervisor:
(Member)

Dr. Farida Chowdhury

Professor
Department of Computer Science and Engineering
BRAC University

Co-Supervisor:
(Member)

Dr. Jannatun Noor Mukta

Assistant Professor, CSE
Director, BSDS
United International University

Co-Supervisor:
(Member)

Md. Tawsif Shahriar Dipto

Lecturer
Department of Computer Science and Engineering
BRAC University

Thesis Coordinator:
(Member)

Dr. Md. Golam Rabiul Alam

Professor
Department of Computer Science and Engineering
BRAC University

Head of Department:
(Chair)

Dr. Sadia Hamid Kazi

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

Abstract

With the growing use of digital devices in Bangladesh, cybersecurity risks such as phishing, malware and data breaches have become increasingly common especially among the non-CS background university students in Bangladesh who often lack both awareness and motivation to learn about online safety. Existing cybersecurity training tools mostly target professionals or computer science students, leaving a gap for accessible and engaging approaches for non-technical university students. To address this, our research applied Human-Centered Design (HCD) principles along with the Octalysis Gamification Framework to develop an interactive visual-novel game called "The Exiled Prince" which presents real-world cybersecurity threats through storytelling, decision making and in game quizzes to create an enjoyable learning experience. A controlled study was conducted with two groups where one group is the control group (n = 20) using a traditional tutorial and another group is the experimental group (n = 20) who played the game to measure effectiveness. The game group demonstrated higher engagement, stronger awareness and better knowledge retention compared to the control group. This study contributes to a Human-Centered gamified learning model designed for non-CS university students, demonstrating that game-based learning can make cybersecurity education both effective and enjoyable.

Keywords: HCI, Human-Centered Design, Gamification, Cybersecurity Awareness, Game-Based Learning, Educational-Tool

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction

The technological advancement in the modern era is a double edged sword. As we shift more focus towards digitizing almost every aspect of human life for comfort and ease of access, new threats have emerged. Cybersecurity risks, privacy concerns, rise of mental health issues, job displacement due to automation and Artificial Intelligence transforming the workspace, impacting job roles across major industries - are a few examples that raise concerns for individuals and organizations.

In today's rapidly evolving digital world, cybersecurity threats are increasingly prevalent, making it crucial to equip individuals with the knowledge and skills necessary to navigate the online environment safely. Among the most vulnerable populations are university students, who often lack sufficient awareness of the risks associated with online activities and how to protect themselves from cyber threats [16][63][73]. Such knowledge and awareness is cultivated among employees of organizations through professional training, but those tools are inapplicable for students [5][42]. Traditional methods of cybersecurity education for students include lectures and written materials [5][30][85]. But have proven to be insufficient in engaging and retaining students' attention. Research on this matter suggests that gamification is better than the flat information learning approach (interactive book) and provides better student engagement and post-training performance [55]. Similar results can be found in the implementation of Gamified Intelligent Cyber Aptitude and Skills Training (GICAST) course by The Open University [74]. The research shows that GICAST training is widely acceptable to an undergraduate student population with positive sentiment towards the proposed gamified training session, and indeed produces strong gains in cybersecurity. Gamification has potential as a valuable learning tool that can be employed even more broadly. After GICAST training, post-training levels of knowledge, attitudes and behavior may be seen on par with the levels seen in trained employees in the workplace.

Thus, we suggest using the gamification approach to create engaging scenarios for students, providing an alternative way for information security awareness.This thesis explores the potential of gamification as a solution to enhance cybersecurity awareness among non-technical students in Bangladesh. By developing a digital game tailored to their needs and interests, this research aims to provide an engaging and

interactive learning experience that not only increases knowledge but also encourages behavior change. Through this approach, the thesis seeks to contribute to the growing body of research on innovative educational methods and offer a practical solution to improving security awareness of the students from non-technical background in Bangladesh. In our research, we discuss the theoretical foundations of our gamification approach, the current state of cybersecurity awareness, the design and development of a digital game as a tool to improve security knowledge among students and evaluation through pre-assessment and post-assessment to evaluate if there is any enhancement in the knowledge.

1.2 Motivation

Despite the growing risks, many university students still lack a solid understanding of cybersecurity principles and practices, leaving them susceptible to online attacks such as phishing, identity theft, and malware infections [16][73]. Additionally, there are many challenges to implement security training programs as many often lack motivation or encouragement to participate in such programs [35][51][63].

In recent years, gamification has emerged as an innovative approach to education, leveraging the motivational aspects of gaming to enhance learning experiences. By transforming cybersecurity education into a more interactive and enjoyable process, gamified learning has the potential to increase the users engagement, retention, and behavioral change [35][60][87]. However not all gamification approaches are applicable for students. For example, Riskio-a serious board game in which the players gain knowledge of cyber security assaults and defenses as they play as both the attacker and defender in turn[42]. It showed very promising results in training employees but for students it failed to receive the same reception as they found the game very lecture focused and tedious. Another study suggests that there are negative relationships with regards to the game elements of gamification training programs and learning outcomes[62]. It is important to incorporate the right game elements to have a positive impact on the training outcomes.

Thus, this thesis is motivated by the desire to explore the effective use of gamification using appropriate game elements for students to maximize motivation and engagement.

1.3 Problem Statement

Bangladesh has reached over 131 million internet users by the end of December, 2023 [76]. This number was boosted by the covid-19 pandemic, cornering many services and infrastructures to move their operations online. We should expect active users to increase more as technology becomes more readily available for everyone. But many people are still unaware of the dangers of cyber attacks threatening loss of personal data, credentials, financial loss and so on [5][15][17][19].

The students of our country hold a crucial role in securing our digital safety in the future. The increasing reliance on digital platforms for education, social interac-

tion, and daily activities has made students in Bangladesh more vulnerable to cyber threats. But many of the students are not well educated on this matter to safeguard their cyber security. A study surveyed Bangladeshi people suggested there is a necessity of including cybersecurity education as most of them are ignorant and unaware of basic cybersecurity knowledge [18]. Streamlining cyber security training programs in the education system would make our students become conscious of cyber issues, preparing them for the harsh demand of the current job market. Another study suggests there is a severe cyber security awareness gap among university students as many of them engage in unsafe online activities such as- downloading files from untrusted sources, using unlicensed and out-of-date softwares, improper password habits and so on [73]. Therefore, this thesis aims to develop a solution to improve cybersecurity awareness and knowledge among students in Bangladesh.

1.4 Research Questions

We aim to foster a deeper understanding of cybersecurity among students in Bangladesh. Our objective is to create an engaging, interactive learning experience to grab students attention and bridge the gap in cybersecurity education, fostering better preparedness among students to recognize and mitigate online security threats. By developing a digital game tailored to the specific needs of Bangladeshi students, this research aims to create an engaging tool that not only increases awareness but also empowers students to take proactive measures in securing their online presence. This approach offers a scalable and impactful solution to a critical problem in today's digital age. With our research we aim to answer the following research questions-

- **RQ1 :** What is the current level of cybersecurity awareness among university students?
- **RQ2 :** How do gamified learning methods compare to traditional methods in engaging university students?
- **RQ3 :** What gamification strategies are effective in improving cybersecurity awareness among university students?
- **RQ4 :** What learning goals are targeted by the implementation of gamification strategies?
- **RQ5 :** What is the audience perception toward gamification?
- **RQ6 :** What is the perceived usability of the game among the audience and how does this influence their willingness to complete the security awareness training?
- **RQ7 :** How likely are the audience to apply the knowledge and strategies learned from the game in their personal and academic digital lives?

All of the research questions will be answered in the discussion part with the findings and all we got.

1.5 Research Contribution

Our research contributes to the field of cybersecurity education by developing and evaluating a human-centered, gamified learning experience created for non-technical university students in Bangladesh. The goal of this study was to make cybersecurity learning more engaging, relatable, and effective for students who often find traditional materials too technical or uninteresting. The key contributions of our work are outlined below.

1. **Game Design and Implementation**: The first and most significant contribution is the design and development and implementation of a human-centered gamified game. We created a visual-novel style digital game titled The Exiled Prince, built on Human-Centered Design (HCD) principles to ensure accessibility and enjoyment. Through storytelling, player choices, and interactive quizzes, the game turns complex cybersecurity concepts into meaningful, story-driven experiences that reflect real-world situations faced by students. After designing the game we have successfully implemented the game. The implementation helped us not only to assess our game but also helped us to gather valuable insights about the game for future improvement.

2. **Gamification and Learning Integration**: Our game is the integration of gamification frameworks and learning theories. We brought together the Octalysis Gamification Framework and Constructivist Learning Theory to design gameplay that motivates, rewards curiosity, and reinforces learning through interaction. This thoughtful integration helps the game move beyond entertainment—it supports genuine understanding and lasting behavioral change toward safer digital habits.

3. **Context-Specific Educational Model**: Our game addresses the context-specific educational game for Bangladesh. While many cybersecurity awareness games exist internationally, few address the cultural, educational, and technological context of Bangladeshi learners. By adapting the game's design, tone, and scenarios to fit the local environment, we created a learning experience that feels relevant and relatable to our target audience.

4. **Evaluation and User Analysis**: We have conducted comprehensive evaluation and also executed user-centered analysis. To assess the game's effectiveness, we conducted a controlled study comparing our game with a traditional text-based tutorial. The results revealed that students who played The Exiled Prince were noticeably more engaged, retained knowledge more effectively, and felt more motivated to apply safe cybersecurity practices in their daily lives. These findings show how interactive storytelling can turn complex cybersecurity topics into something relatable and easy to understand.

5. **Sustainable Cybersecurity Education**: The final thing we focused on is promoting sustainable cybersecurity education. We show that story-driven digital games can serve as lasting educational tools within academic settings, keeping learners interested and involved over time. Since the game's framework

is both flexible and scalable, it can be adapted to address emerging cybersecurity issues, different learner groups, and various cultural contexts. In this way, The Exiled Prince stands not just as a single educational game but as a foundation for future gamified approaches to cybersecurity learning.

1.6 Thesis Structure

We have completed the rest of the research in the following chapter:

Chapter 2 (Literature Review): It discusses existing research on cybersecurity awareness, complexness of existing methods in teaching cybersecurity knowledge, popular digital threats (password protection, phishing, identity theft, malware, cryptojacking malicious popup ads, ransomware) as well as the application of gamification in teaching. It contrasts gamified versus non-gamified methods, surveys relevant games, and detects gaps in cybersecurity training for students, particularly those from non-technical backgrounds. The chapter concludes by positioning our project as a unique gamified solution designed for Bangladeshi university students.

Chapter 3 (Methodology): This chapter describes our research methodology, starting with the target participants and research questions, then moving on to solution design. It discusses why a Visual Novel style was chosen, defines the constructive learning principle and the Octalysis framework for gamification, and explains how these theories informed the development of our game The Exiled Prince. It ends by presenting the evaluation plan, which uses user studies to measure effectiveness.

Chapter 4 (A Gamified Solution: The Exiled Prince): This chapter provides the details of the game's design and development. It outlines the chosen development stack, game components, deployment on Netlify, and the narrative framework. The chapter breaks down the story into interactive decision points, incorporates in-game quizzes, details the game mechanics, maps learning outcomes to Constructivist Learning Theory, and shows how Octalysis core drives are embedded in the design.

Chapter 5 (Game Evaluation): This chapter reports on the evaluation of The Exiled Prince through a structured user study. It covers participant demographics, pre and post-assessment procedures, study activities, and data collection. The analysis combines quantitative measures (e.g., knowledge gains, usability) with qualitative insights (user feedback on motivation, engagement, and learning). The evaluation provides evidence of the game's effectiveness in boosting cybersecurity awareness and influencing student behavior. Also data evaluation process of this focuses on which method is actually better or not. The whole prove was done by hypothesis testing in this chapter.

Chapter 6 (Discussion): This chapter discusses about the findings and all the analysis. This chapter is focused on answering the research questions. All of seven research questions has been answered based on the finding of our study in this chapter.

Chapter 7 (Conclusion): The final chapter summarizes the research findings, highlighting how gamification enhanced student engagement with cybersecurity education. It reflects on the strengths and weaknesses of The Exiled Prince and suggests future

directions, such as expanding the range of threats addressed, adding multiplayer collaboration, and adapting the solution for audiences beyond Bangladeshi university students.

Chapter 2

Literature Review

The chapter discussed about the existing literature which are related to the cybersecurity awareness, digital threats and use of the gamification method as educational approach. The chapter also discussed about the threats that we have worked on in our game. By analyzing the current trends, gaps and challenges in cybersecurity education specifically for the non-CS University students of Bangladesh this chapter helps us to establish a context as well as rationale for developing our proposed learning based gamified solution.

2.1 Preliminaries

Cybersecurity has become a critical focus in the modern digital landscape as cyber threats continue to evolve, posing significant risks to all end users of digital devices. The need for effective cybersecurity awareness and training programs is rising as sophistication of cyber attacks is racing with the evolution of cybersecurity. Then, the review is categorized into 4 key areas: Cybersecurity Awareness and Education, Cybersecurity Threats and Trends, Gamification in Cybersecurity, and Gamified and Non-Gamified Approaches. By examining these sectors, we aim to highlight the importance of cybersecurity education and the potential of gamification in enhancing training effectiveness, engagement, and ultimately, cybersecurity preparedness.

This review provides essential background information to help readers understand the context behind our problem statement and research objectives of this study. Through this exploration, we would assess how gamified methods may serve as a viable solution to address current challenges in cybersecurity training and awareness. Cybersecurity awareness involves understanding potential risks like phishing, ransomware, identity theft,malicious website, password protection, and the growing prevalence of cyber crimes, while education focuses on improving practices to avoid these threats. In designing an effective gamified approach to cybersecurity education, it is essential to identify and incorporate threats that are both highly relevant to learners' digital experiences and frequently cited as areas of weakness in academic literature. Based on a comprehensive review of existing studies and several common cybersecurity threats we decided to address the following cyber threats in our research-

2.1.1 Weak Passwords

Weak passwords are one of the most common vulnerabilities exploited by cyber attackers. They often include easily guessable elements like “123456”, names, or repeated characters. Poor practices such as reusing passwords across accounts, failing to update them regularly, or using short and simple phrases leave users susceptible to brute-force and dictionary attacks. Surveys reveal concerning practices among students. For instance, 53% of students reported having stronger passwords for banking compared to social networking accounts, indicating inconsistent application of security habits [27]. Moreover, 69% of students admitted using personal information in their passwords, making them predictable and easily guessed [14]. Alarmingly, 34% of students never change their passwords and 44% only sometimes update them [14]. Such behaviors highlight the widespread prevalence of weak password practices, even among educated populations. This underscores the need for interventions like gamified training tools that simulate the consequences of poor password hygiene and encourage stronger, more secure habits.

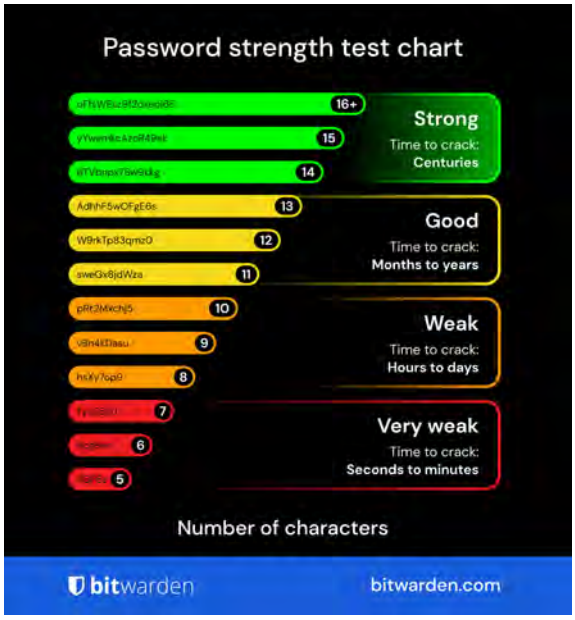

Figure 2.1: Password Strength

Various Studies highlight insecure practices such as using personal information in passwords, lack of password updates and so on are prevalent among many university students, even those with a CS background. This careless habit makes them easy targets for attackers, underscoring the need for improved behavior through interactive learning tools that simulate consequences of poor password hygiene. Figure 2.1 is the demonstration of weak passwords and strong passwords.

2.1.2 Ransomware

Ransomware is a type of malware that encrypts a user’s files or locks their system, demanding payment in exchange for a decryption key. The user gets messages like

Figure 2.2 after a ransomware attack. It can cause irreversible data loss, financial damage, and operational disruption, especially when backups are unavailable or compromised. The scale of ransomware in education is striking: in 2022, 65 ransomware attacks targeted schools and colleges, affecting 1,436 institutions and disrupting the education of nearly 1,074,926 students [39]. These incidents highlight how devastating ransomware can be in academic environments. Gamification literature emphasizes the importance of exposing learners to high-stakes, real-world scenarios. Including ransomware in training simulations addresses both behavioral and technical gaps, ensuring students are aware of the severe consequences of ignoring preventive measures such as software updates and backups.

Figure 2.2: Ransomware

Gamification literature emphasizes the importance of exposing learners to real-world scenarios. Ransomware threats in simulations help players experience the high-stakes consequences of failing to update software, clicking unsafe links, or ignoring antivirus protocols. Including ransomware in the game addresses both behavioral and technical gaps, as students often underestimate the severity of these attacks. After getting attacked by ransomware the users get the messages which is shown in the Figure 2.2.

2.1.3 Identity Theft

Identity theft occurs when someone unlawfully obtains and uses another person's personal information—like social security numbers, login credentials, or banking information—for malicious purposes. This can lead to unauthorized financial transactions, fraudulent accounts, or impersonation. Students often underestimate these risks. Studies indicate that 69% of students were unaware of identity theft on social networks, often oversharing personal data online without recognizing the consequences [21]. This behavior reflects a lack of perceived personal responsibility for maintaining digital safety, with many assuming cybersecurity is the organization's role rather than their own. Gamified scenarios highlighting oversharing and its consequences can help learners understand accountability and develop vigilance against identity theft.

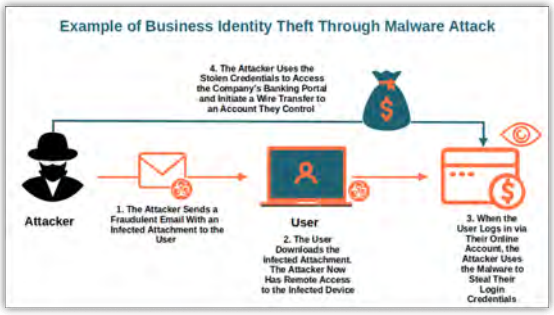

Figure 2.3: Identity theft

University students frequently share personal data online without fully understanding the risks. Studies report a low level of perceived personal responsibility in maintaining digital safety, with many students assuming cybersecurity is the organization's job. Identity theft scenarios in a game can effectively illustrate the personal consequences of oversharing or careless online behavior, reinforcing accountability and vigilance. The Figure 2.3 shows how identity theft works.

2.1.4 Phishing

Phishing involves tricking users into revealing personal information, such as login credentials or financial details, by impersonating trustworthy entities through emails, messages, or fake websites. Phishing remains one of the most effective and widespread social engineering techniques used to compromise user data. Empirical evidence highlights the scale of the issue: one experiment revealed that 77% of participants fell victim to phishing attacks, with students making up 41% of the victims [37]. Similarly, a large survey of 498 students in the US Pacific Northwest found that 50% could not define phishing and 55% could not define malware, showing clear knowledge gaps [17]. Given that phishing exploits human behavior more than technical flaws, it is highly relevant for inclusion in gamified training contexts where simulated scenarios help learners practice critical thinking and detection skills in realistic settings. Just like Figure 2.4 attackers target for the sensitive info of the user.Phishing is a recurring topic in gamified tools reviewed in the literature—games like Anti-Phishing Phil and Phishy were specifically designed to train users to recognize suspicious URLs, deceptive subdomains, or urgent scam messages [4][23]. Given that phishing exploits human behavior more than technical flaws, it is highly relevant for inclusion in a gamified training context where simulated scenarios help build critical thinking and detection skills.

Figure 2.4: Phishing

2.1.5 Malware

Malware is one of the most common threats of the cybersecurity world. In this threat malicious scripts stay hidden inside the cracked or free software. Later on, it causes problems with the device. People usually face this attack because of downloading crack version of paid software from unknown and untrusted websites. Just like Figure 2.5 malware is corrupted scripts hidden inside a cracked software. Studies show that a significant number of students—68% of IT/cybersecurity students and 80% of CS students—download files from untrusted sources, indicating poor discernment of website legitimacy [73]. Because of this reason they remain vulnerable to the threat of malware.

Figure 2.5: Malware

2.1.6 Malicious Pop-up Ads

Pop-up ads are often used as a delivery method for social engineering attacks or malware. They may trick users into clicking "urgent" warnings or fake software updates, which can lead to drive-by downloads or data theft. Pop-up ads are common online nuisances and often the first interaction students have with potentially malicious content. Despite their ubiquity, learners tend to underestimate the risks, especially if the ads mimic real system notifications. Simulating these in a gamified setting allows users to practice identifying deceptive pop-ups and avoid reactive, risky behavior.

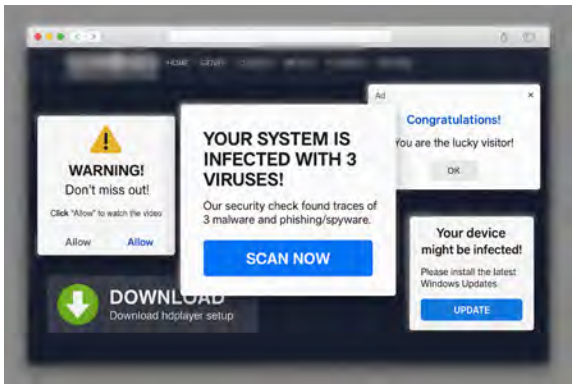

Figure 2.6: Pop up ads

Pop-up ads are common online nuisances and often the first interaction students have with potentially malicious content. Despite their ubiquity, learners tend to underestimate the risks, especially if the ads mimic real system notifications. Simulating these in a gamified setting allows users to practice identifying deceptive pop-ups and avoid reactive, risky behavior. The Figure 2.6 shows how pop up ads look like.

2.1.7 Cryptojacking

Cryptojacking occurs when malicious software secretly uses a victim's computing resources—such as CPU or GPU power—to mine cryptocurrency without their consent. Unlike ransomware, cryptojacking does not lock files but instead silently drains system performance, causing overheating, slowdowns, and hardware damage over time. Recent reports show that XMRig, a cryptomining malware, was used in 65% of cryptomining attacks in 2023, with attackers increasingly integrating additional malicious functionalities and targeting platforms with enhanced GPU capabilities [80]. Figure 2.7 is a representation of cryptojacking.

Figure 2.7: Cryptojacking

Students are particularly at risk due to frequent downloads from untrusted sources, shared university networks, and reliance on high-performance devices for graphics, design, or engineering coursework. In educational contexts, cryptojacking scenarios in games can help learners recognize unusual performance symptoms, understand the risks of unsafe downloads, and practice safe online behavior to reduce exposure to stealth-based attacks.

Now we will explore the intersection of cybersecurity threats, awareness, and the use of gamification in training by reviewing existing papers based on the following search

criteria- Gamification, cybersecurity awareness,Use of gamification in cybersecurity, serious games, security awareness training (SAT), cybersecurity in education, gamification for students etc

2.2 Review of Existing Research

2.2.1 Cybersecurity awareness and education

Cybersecurity awareness is one of the most essential elements to tackle all the digital threats. As the human risk factor is the most prevalent threat in cybersecurity, raising awareness protects the end-users from the digital threats and improves their online behavior. However people are still not educated enough and aware about the digital threats and security practices. Ahmed et al.[18] conducted a survey in their study and found that 61% of users only take basic precautions like verifying website legitimacy, insecure practices remain prevalent, such as 69% using personal information in passwords. Even though some people still rely on newspapers (72%) and online platforms (63%) for updates about cyber crimes, 65% of them believe that existing laws for cyber crimes are not effective to tackle cyber crime effectively. Similarly, Ferdous et al.[93] mentioned about a survey where among 545 respondents 80% of respondents claimed not to have experienced cyber attacks, and only 9.4% reported incidents, which indicates lack of awareness and action towards cyber crimes. While most users identify as intermediate (61.8%), their cybersecurity practices are not enough to protect themselves from cyber threats, only 8% use antivirus software and 9.7% rely on software updates. It also shows Generation Z's tendency to share personal information online, which significantly increases their vulnerability. Security habits, such as reading terms and conditions, are also less and only 31% sometimes review them. Furthermore, Kundu et al.[26] talked about the authors also mentioned about the changing legal environment of the country, which is putting in place laws like the ICT Act 2006 and the Draft Digital Security Act 2016 to fight cyber crime. However there is a problem with implementation.

Additionally, Kshetri, Vasudha, and Hoxha[73] discuss the awareness of cybersecurity among university students, comparing three groups: CS, IT/Cybersecurity students, and others. In total, 150 students were surveyed and surprising gaps were identified in the safety of online behavior. In the results 68% of IT/Cybersecurity students download files from untrusted sources, and as many as 80% of CS students and 72% of non-CS students did so. Among the CS and non-CS students, 16%, and of the IT/Cybersecurity ones-12% simply allow their software to be out of date. Such was going on with password habits. None of the CS and IT ones change their passwords on a weekly basis; only 8% of non-CS students do. 48% of CS students, 36% of IT/Cybersecurity students, and 52% of non-CS students never or rarely change their passwords. Internet use is now a big part of daily life, with 24% of IT students surfing online for over 10 hours a day compared to 16% of CS students and 8% of non-CS students. The vast majority of the students, 84% CS and 80% IT students, pay bills online, hence exposing themselves to risks. The shocking part is that 8% of CS students and 12% IT students think it is solely a concern of an organization, and 4% of the non-CS students said the same. Consequently, Li

and Liu[56], focused on how citizens of four countries-Israel, Slovenia, Poland, and Turkey-comprehend and handle cybersecurity. 81% of respondents acknowledged familiarity with cybersecurity through sources like the Internet, only 56% were regularly updating their software, and just 45% were using spam protection. People were very concerned about the threats of violation of privacy (average worry score: 4.20) and loss of data (4.17). Yet, protection measures taken included only basic levels such as antivirus software (75%) and strong passwords (85%). Education did make a difference: students with some training in IT security showed better knowledge on cybersecurity. On the other hand, 66% of participants had never been to such training. Also, Hunt[16], highlights the growing importance of cyber security awareness, particularly in higher education, as students getting familiarized with online platforms, increasing their exposure to cyber threats such as phishing, identity theft, and malware. A significant percentage of students and educators lack basic knowledge of online safety. The paper also mentions many schools are not prepared to teach these cybersecurity skills. For example, malware threats on mobile devices now surpass those on PCs, largely due to unsecure networks and app vulnerabilities. Alotaibi et al.[13] discuss the growing number of cyber crimes, especially in Saudi Arabia, where 66% of the population (18 million people) are internet users but the majority of them have poor cybersecurity awareness despite having good IT skills The authors also attested that humans create poor passwords and use low-quality defenses like antivirus, but most of them embraced the idea of using mobile games as a means of awareness. Serious games as fun yet interactive education and training tools emerged as appropriate to cybersecurity educational and training endeavors. Also, Morais et al.[63] says that most of the student don't know how to implement gamification tools in real life and most of the students have good cybersecurity habits, such as strong passwords but lack regular password updates or advanced knowledge. Some students reported being victims of cyber attacks(phishing or ransomware).

Even though the importance of security awareness is quite important but existing education approaches have significant limitations. Existing security courses often require previous knowledge in different fields which make them inaccessible for non-technical background students. Existing online tutorials also provide incomplete information with so small context. Also, short training sessions fail to facilitate deep learning, reflection or repeated practice [5]. Furthermore, complex security interfaces and too much technical guidance some times overwhelm non-technical users which eventually leads to fear, helplessness and security fatigue [30]. Additionally , traditional methods are boring and irrelevant and also the knowledge does not ensure the correct behavior. Because of this, non-technical users remain vulnerable to the cyber threats [85].

This review indicates that, even though the number of cyber crimes is increasing day by day, people are not well educated to combat these threats. Thus cyber crimes pose a significant risk impacting our goal to create a safe Digital Bangladesh. Cyber awareness training should be a mandatory procedure in our education system to improve awareness among the students. However the existing materials are complicated for non-technical users.

2.2.2 Cybersecurity Threats & Trends

Cyber threats are continuously increasing and it is continuously putting challenges for the users as well as for an entire nation. The Human Risk Review 2024 report lists the following tactics as the most successful in cyber attacks-1. Phishing, 2. Malware, 3. Ddos, 4. Ransomware, 5. Social engineering attacks beyond phishing and vishing.

Multiple research papers highlighted the cyber threats in Bangladesh with the number of internet users reaching 131 million by 2023. Kundu et al.[26] has stated about the rise of cyber crime in Bangladesh, focusing on its financial sector, where 52% of banks face high security risks. Another research also mentioned cyber propaganda cases like the 2012 Ramu violence, where a fake account in Facebook incited violence across the country, exposing the citizens low cybersecurity awareness. Surveys indicate widespread exposure to cyber threats, with 77% of participants experiencing phishing, 71% facing identity theft, and 80% encountering malware. Both [26] and [18] mentioned about the major incidents like the 2016 Bangladesh Bank Heist, resulting in a $81 million theft due to malware exploiting system vulnerabilities. However, only 40% reported such incidents, often due to ignorance, fear, or distrust in the process. Furthermore, Sharif and Ameen[51] stated about 45% of the US population was compromised by the Equifax breach of 2017, and 300,000 computers worldwide, including 19,000 healthcare appointments in the UK, were canceled due to the WannaCry attack.

In another study Li and Liu[56], talks about the growing dangers of cyber-attacks and how cybersecurity is becoming more important nowadays. The paper talks about cyber-attacks, like hacking, phishing, malware, and botnets, targeting important systems like government networks, businesses, and even individuals. These attacks can happen anywhere because cyberspace connects the whole world, making it hard to stop them with traditional methods. A big issue is that there's no clear, agreed-upon definition of what a cyber-attack is, which makes it harder for countries to work together and enforce laws. Additionally Fatokun et al.[93] discussed the crucial role of cybersecurity knowledge and behavior in addressing the growing threat of cyberattacks.It also mentions that human mistakes are responsible for 70–80% of the damage caused by cyber attacks. Common mistakes, such as clicking on phishing links, using infected USB drives, or ignoring security updates, highlight the vulnerability of users despite advancements in technical solutions. It explains that current security systems overlook the fact that people have varying levels of technical skills and understanding, leading to gaps in their effectiveness and leaving users more vulnerable to cyber threats.

Cyber threats are continuously growing in this modern and digital era. Users and organizations are continuously facing different threats in their daily lives. Users must need to be educated to tackle all these cyber threats.

2.2.3 Gamification in Cybersecurity

Gamification has been one of the effective and emerging ways of education. It has also been effective in cybersecurity education. Sharif and Ameen[51] has stated gam-

ification as a promising method to educate users about security threats and improve compliance. Traditional methods like text-based training and generic education programs are criticized for their lack of engagement and personalization. Gamified tools, in contrast, create interactive and engaging learning environments, addressing the human factor—identified as the main vulnerability in cybersecurity.. In another paper Scholefield and Shepherd[35] focuses on increasing cybersecurity awareness using gamification. Some learning Methods were shown, but which were not for long-term process and not effective. According to participants, the game was enjoyable and helpful in increasing their knowledge about password security. Another study on Scenario-based eLearning suggests such gamified approach introduces active learning strategies such as problem-based or case-based learning by using interactive scenarios [32]. The students found the scenarios more enjoyable for their learning experience improving their thinking skills and their engagement with the content was high due to relevance to real life components.Also, Juho Hamari, Jonna Koivisto and Harri Sarsa (2014) [10] examines previous research to understand how game-like elements such as points, badges, and leaderboards influence user motivation and engagement. After reviewing several empirical studies from fields like education, business, and health, the authors found that gamification often leads to positive outcomes, increasing participation and motivation.

Furthermore, in an article Williams et al.[87] found the role of gamification and game-based learning in cybersecurity education. Mainly non-technical students and developing their skills. Also this paper proposes an effective solution to overcome the limitations of existing platforms. Additionally, in another article Hendrix et al.[15] analyzes the effectiveness of serious games for cybersecurity education through a structured literature review and product search. 28 papers were analyzed where general cybersecurity awareness(7), network security (6), phishing (4) and 3 on end-user PC protection. While only 3 studies addressed professional training in areas like insider threats and forensics. Out of these, 6 studies lacked evaluations, 6 had superficial evaluations, and only 11 provided measurable outcomes. Additionally, 15 games were identified, including PBS Cybersecurity Lab, most of which targeted children, teenagers, and students, with very few designed for professionals. In this paper found that most games are short-term and lack long-lasting behavioral impact. Also, Xiao et al.[78] explores how using games can improve cybersecurity education in colleges and universities, especially in China. It highlights the rise in cyberattacks and points out issues in current teaching methods, like outdated materials, lack of hands-on learning, and boring approaches. Additionally Fatokun et al.[60] has proposed to develop a gamification model that will help students improve their awareness and behavior about cybersecurity in their paper. They tried to show that using gamification correctly increases cybersecurity knowledge and reduces risky behavior.

Gamification is suggested as a way to make learning more fun and effective by using interactive and immersive games. These games can simulate real-life cybersecurity challenges, helping students learn by doing. By making cybersecurity education more engaging and practical, students can better understand and handle cyber threats. The following sections cover a few examples of research on different types of existing gamification approaches.

Role playing games

In another paper Scholefield and Shepherd[35] have developed an Android-based role-playing game (RPG) and tested it with 17 participants to improve password security. The game incorporated gamification elements such as characters, leaderboards, time pressure, and feedback, which made the learning process engaging and effective (RPG).

Also, a game RAD-SIM was introduced by Thompson et al. (2022)[65] focuses on promoting critical thinking through role-playing (Mentalizing), setting clear learning goals (Response/Attack), designing games suited to the audience (Design), encouraging teamwork and competition (Sociality), using rewards and confidence-building and (Incentives). While developed for cybersecurity, RAD-SIM can be applied to other fields to improve learning outcomes. The authors recommend further testing and real-world application to refine this method.

Capture the Flag (CTF) games

Williams et al. proposes two games (1. open-ended CTF 2. story-based CTF). open-ended CTF enhances student teamwork, critical thinking and problem-solving skills. On the other hand, story based CTF makes the learning experience more engaging through a series. 80 students participated, divided into 6 groups. These games are particularly helpful in reducing the complexity of cybersecurity and helping students acquire skills through realistic challenges. Final result was very good, games increased student interest in cybersecurity and helped to create an inclusive learning environment (CTF).

Serious games

Alotaibi et al. (2016)[13] has talked about serious games which have been identified as interactive education and fun tools to increase cybersecurity awareness. "Anti-Phishing Phil", which instructed users on how to recognize phishing attacks, while most of the studies were small or pilot studies. Another paper introduces two educational tools, an interactive book and a board game aiming to solve the lack of efficiency in information security awareness training[61]. They suggest that the board game approach is better than the flat information learning approach (interactive book). It indicates that gamification provides an alternative way for information security awareness training in a fun and educational way.

Rikkers and Sarmah [90] created a serious game that teaches students how to prevent USB-based cyber attacks. The game is a story-driven interactive novel made with Twine. In this game players step into the role of a cybersecurity investigator trying to uncover the cause of a ransomware incident.Instead of relying on leaderboards or points, the game focuses entirely on storytelling using relatable characters, realistic situations and multiple possible endings to make the learning experience more engaging and memorable.The study involved 28 university students where students had both technical and non-technical background, aged between 18 and 25. They played the game and completed surveys before and after to measure their engage-

ment and how much they learned.The results were clear: the story driven approach helped students better understand USB-based attacks, stay engaged, and connect cybersecurity lessons to real-world situations. Compared to traditional videos or other training methods, the story based game was found to be more enjoyable and effective.In the end, the authors showed that story-driven serious games can make cybersecurity learning feel more human and relatable, turning abstract technical lessons into experiences that are both educational and genuinely enjoyable.

Riskio is a serious board game in which the players gain knowledge of cyber security assaults and defenses as they play the role of both the attacker and defender[42]. It helps them understand the impact of their actions on important assets in a hypothetical organization scenario. They tested the game on employees and graduate students to determine Riskio's is more suited in raising cyber security awareness for the employees as they were able to relate to the given scenarios. Similarly, Perihack is another serious game aiming to improve cybersecurity awareness from both attackers and defenders point of view[59]. Their study on this game suggests that the attacker gains a better understanding of the nature of cyber attacks, how it is initiated and its evolution. The defenders see the value of managing various weaknesses with limited resources and information.

Hilliard et al.[84] has discussed the effectiveness of ARP Adventure. ARP Adventure is a serious gamified tool which was designed to enhance engagement and mastery of Address Resolution Protocol (ARP) concepts in cybersecurity education. Pre- and post-survey data showed a 27% increase in interest in ARP (from 64% to 91%) and a 9% rise in concern about cybersecurity incidents (from 82% to 91%), this highlights the game's ability to boost interest in the subject matter. The game gained 100% engagement, with 91% of the participants enjoying it and finding it an effective learning tool. Confidence in the ARP-related topics increased significantly, with mastery of complex concepts such as Frame Payload and Frame Check showing up to 73% growth, while foundational concepts such as Router and Protocol definitions improved by 10-20%. The updated version of the game, featuring enhanced interactivity, usability, and randomized question design, addressed prior criticisms, such as sluggish controls and limited engagement. Students also praised its ability to present information interactively and repetitively, aiding retention, and many expressed willingness to use the game for leisure as well as learning.

A competitive, mobile-friendly quiz, a serious game was developed by Nijland[64] with features like scoring, timers, leaderboards and instant feedback. Two surveys were conducted: one with 29 students to refine the game, and the other with 24 students (split into trained and untrained groups) to test its effectiveness. Trained students also completed with fewer errors (1.7% vs. 4.2%) and answered more quickly (39s vs. 93s). While students liked playing the game (average rating 3.7/5), they suggested more challenging and varied questions through feedback. The game shows promise but requires more diverse participants and additional features like adaptive difficulty and social features.

Simulation based game

Ask et al[53] has presented a mode which aims to build skills in meta-cognitive awareness, perspective-taking, and explicit communication of Recognized Cyber Pictures (RCPs). Gamification features, including storytelling features, points (up to 100 per step), feedback, and self-assessment, promote engagement and adaptability was added in this model. The five steps in the training process are pre-task surveys, scenario-based cyber tasks, OLB-facilitated RCP communication, expert-reviewed situation reports, and continuation of the task with feedback loops. There are points for completion of milestones (10 points for each), with multipliers (1-5) based on memory load. Outcomes show potential benefits, for instance, 50% reduction in decision errors, up to 80% less communication errors, and 50% improvement in situational awareness. Supported by the Norwegian Research Council (#302941), the model will align mental models across teams and bridge essential gaps in cybersecurity training.

Different types of gamified models and tools are helping users to educate and understand the situations during cyber attacks. These types of games help them to increase their knowledge as well as these types of games can entertain them.

2.2.4 Gamified vs. Non-Gamified Approaches

In modern days gamified methods are enhancing knowledge more effectively than the non gamified or traditional methods. Morais et al.[63] mentioned in their paper that students clearly understand gamification and its goals regardless of their higher education course. They also mentioned that gamification has potential as an effective tool for enhancing cybersecurity awareness. Another paper suggests that training with Scenario-based games creates an engaging training environment in which students face real life work challenges in simulated scenarios and receive realistic feedback as they advance[55]. Unlike traditional training in which students gain knowledge through literature text , students in scenario-based training are more inclined to actively engage in the process from start to end. This allows students to learn from failures, ultimately adjusting their approaches until they succeed.

Furthermore, Kijpoonphol and Phumchanin[25] compare two different ways of teaching to 10th-grade students in Thailand in their paper. One is traditional teaching and the other one is gamified teaching (using games). It divides the students into two groups. One group learns using the traditional method (control group), while the other group learns through games (experimental group). The results show that the gamified group performed better on the post-test. Their average score was 8.14, while the traditional group's score was 5.50. This was a significant difference, meaning the gamified teaching method helped students understand and remember phrasal verbs more effectively. The gamified group improved their scores by 6.49 points, while the traditional group only improved by 4.25 points. When it came to how satisfied students were with their learning, the traditional group gave a slightly higher satisfaction score (3.84) compared to the gamified group (3.54). The study shows that games can be a powerful way to help students learn and remember new words. Similarly, another research introduces two educational tools, an interactive

book (traditional) and a board game (gamified) aiming to solve the lack of efficiency in information security awareness training[55]. Two different groups were given these tools to assess their learning experience using a pre-post design. The post training result suggests that the board game approach is better than the flat information learning approach (interactive book) and provides an alternative way for information security awareness training in a fun and educational way.

Additionally, in another paper Steen and Deeleman[58] has shown that whether a cybersecurity-focused serious game could improve cybersecurity attitudes, perceived control, intentions, and behavior compared to a standard game with or without cybersecurity information. The study involved 258 participants, with 89 playing the cybersecurity game, 80 playing the control game with cybersecurity information, and 89 playing the standard control game. Results showed that those who played the cybersecurity game reported higher cybersecurity awareness, confidence in applying security measures, and intentions to follow best practices. Compared to the control groups, they also demonstrated better self-reported cybersecurity behavior, such as checking emails for phishing and locking their screens. Additionally Ros et al.[50] analyzed how the game Max and Dr. Manhaussen affected students' learning, confidence, and performance in an online cybersecurity course. Based on cognitive constructivism, the game uses real-life examples and engaging metaphors to illustrate important cybersecurity concepts such as data security and system security. Out of 248 students, 119 (47.98%) played the game, while 129 (52.02%) did not. Data from 69 students and responses from 49 were analyzed using SEM. The results showed that students who played the game performed significantly better, scoring an average of 13.85% higher than those who did not play the game. In addition, the dropout rate of students who played the game was much lower (11.76% vs. 57.37%). Structural equation modeling (SEM) analysis found that engagement and contextualization had significant effects on students' self-esteem and perceptions of the game's effectiveness, which improved their sense of achievement. The game motivated students, helped them understand complex concepts.

All these researches proves that gamified methods are performing better in teaching cyber security knowledge than the traditional or non- gamified methods.

2.2.5 Related Work

Koivisto and Malik[44] analyzed 12 studies of older adults, age 55 and older and revealed that 92% of them examined whether and in what manner gamification can contribute to healthy aging. Specifically, 42% focused on cognitive function, 33% examined physical function, and the rest explored mental function or technology use in older adults. The average participant age was approximately 71, with study sample sizes ranging between 9 and 60, averaging around 33 per study. A significant portion (67%) of these studies involved controlled experiments, comparing intervention groups with non-intervention groups. Half of the studies used tablets for their interventions, while others relied on gaming consoles (25%) or desktop computers. Encouragingly, 83% of the studies reported positive outcomes, including improved memory, enhanced cognitive skills, increased physical activity, greater confidence, and heightened motivation. However, these improvements were gener-

ally minor, likely due to the short duration of the studies or the small sample sizes. While new technology can present challenges, 90% of participants in certain studies were already familiar with computers and the internet. The most common gamification features included progressively increasing difficulty as players advanced, social interaction, point-based systems, and progress tracking. Overall, the findings suggest that gamification can be a valuable tool for older adults, particularly in health-related settings.

There are many games cybersecurity-related games available. All these games fall under different categories. Some of them falls under anti-phising,some of them are focused on password protections. The following sections will cover different type of existing games as well as their categories.

Gamifying Phishing Prevention

Anti-Phishing Phil is an online instructional video game. It instructs on how to recognize phishing URLs, when to look for clues within web browsers, and how to utilize search engines to acquire authentic sites. Existing online, players manage an underwater world and control a fish named Phil who has to consume secure worms hanging on authentic URLs without touching phishing links. With a guiding mentor fish named Phredd, the game offers instant feedback for every decision, and players learn how to recognize suspicious URLs via prevalent phishing clues such as misspelled domains or misleading subdomains[4].

Phishy is an online learning game aimed at enhancing phishing recognition skills for enterprise users. Players guide Sam, who is swimming ashore without falling victim to phishing traps in the form of suspicious links. For three levels of play, users encounter increasingly complex scenarios, and make decisions on whether or not a URL is genuine. Each correct response awards points, and an incorrect response decreases lives and imposes threats such as shark attacks—representing threats such as malware. Immediate feedback allows for easier learning from errors. Its interactive format invites replay, allowing users to enhance their phishing recognition skills incrementally over time[23].

What.Hack is an immersive cybersecurity experience in which players become a security analyst who must prevent a cyberattack. To win, players need to track digital threats by decoding clues, cracking hidden messages, and making strategic decisions. The game combines suspenseful storytelling with puzzle-solving to educate players on essential hacking skills and enhance their cybersecurity capabilities in a hands-on, simulated setting[36].

Persuaded is a single player card game to help people understand the dangers of social engineering attacks like phishing by starting with five cards and eventually drawing one card each round; the card deck is divided into attacks, defense, and action card categories. Attack cards denote attempts of social engineers to lie to the players and identical defense cards prevent attacks and grant points. When a player lacks a good defense, he or she either loses a defense card or a heart (life) and the exhausted attack and defense cards are pushed to the deck rendering it more difficult. Chance cards enable the participants to get a glimpse into the future as well as avoid drawing dangerous cards to avoid imminent attacks. At the event of

all hearts being consumed or the deck is empty, one has lost[22].

Cyber Smart is an edutainment game that will improve the players' awareness and understanding of typical cyber risks including phishing, malware, and passwords vulnerabilities. Cyber Smart delivers real-life inspired scenarios in which the players must make quick but well-informed decisions to safeguard their online identity and data. There are new challenges on each level—such as detecting fake mails, using secure passwords, or detecting malware downloads. Cyber Smart's game mechanic relies on interactive quizzes, narrative-driven storytelling, and timed decisions that promote critical thinking and secure online behavior in an engaging gamification-based game[79].

Secu-One is a gamification-based cybersecurity training tool that raises the awareness of the user through simulated attacks. Users encounter situations such as phishing attacks or suspicious behavior and make the appropriate response choice. Interactive decision-making, real-time feedback, and performance monitoring are employed by the game to sustain learning. The game targets user behavior improvement, with particular emphasis on social engineering attacks[34].

Gamifying Password Security

Hacked Time is an interactive, narrative-based cybersecurity game that sends the protagonist traveling through time to assist a student with an online attack. By using point-and-click controls, users move through scenes, collect clues, and make decisions regarding phishing, password security, and risky behavior. All decisions drive the narrative and yield instant feedback, reinforcing positive cybersecurity practices. The game is intended to raise user confidence and awareness through the medium of interactive storytelling and real-world examples[41].

Internet Hero is an adaptive, story-driven cybersecurity video game in which players go through realistic digital scenarios like phishing, password selection, and malware avoidance. A branched story narrative enables players to make decisions whose consequences control the story. An intelligent tutoring system provides personalized feedback after each decision point, and modular tasks aim for specific cybersecurity competencies. Difficulty adjusts to user performance, and player progress is monitored, with leaderboards for encouraging engagement. Each module is mapped to specific competencies, so it can be tailored for organized learning and competency tests. This game also falls under anti-phising and malware category[7].

Cybersecurity Escape Room is a timed, puzzle-style game in which players solve sequential cyber security puzzles such as phishing, password cracking, and malware analysis to advance levels. Each puzzle imitates threats encountered on the web and demands logical reasoning, cyber clues, or terminal commands. Adaptive difficulties, hints, and quizzes reinforce learning and make it an educational yet engaging experience. This game also falls under anti-phising and malware[66].

Security Empire is a turn based multiplayer game that revolves around the concept of simulating the lives of players who own a virtual green energy company that must be grown but at the same time, the problem of security must be balanced. Players invest in controls and security operations, respond to malware and phishing

attacks and take business decisions to protect assets. The game provides feedback on the practices being used by the players and enables the players to learn the response of security practices on a company in a real sense. Such games also belong to anti-phishing and malware[12].

Gamification in Malware Awareness

CyberVR is a cybersecurity training video game experience of virtual reality that places the players in interactive and immersive 3D environments with which to simulate on-scene cyber attacks. Working on virtual interfaces and objects, players take such actions as running phishing attacks, studying malware, and hardening systems. The experiential learning adopts time bound, hand on problem-solving. CyberVR is a fully developed environment that is intentionally created to train and educate people on the field of work and career in the sphere of cybersecurity. This game can also be classified as an anti-phishing game[52].

Kaspersky Disconnected is a digital visual novel story telling educational game. The game was designed focusing on enhancing cyber security knowledge through storytelling and interactive gameplay. In the gameplay, player go through different scenarios where they must need to respond and detect the cyber attacks like malware threats, phishing attacks and social engineering attacks. The game also provides feedback on decisions immediately. The mechanics include pointscoring, progressive difficulty and guided decision making. The game is suitable for the users with different prior knowledge skills. Kaspersky Disconnected serves as a hands on tool for enhancing the cybersecurity awareness through gamification [43].

CybAR is an augmented reality game engineered to train on cybersecurity with live training. It takes virtual cybersecurity threats to the real-life, allowing players to learn how to overcome such threats as phishing, malware, network breaches on their phones or AR glasses. Incorporating the domains between physical space and digital situations, users learn cybersecurity parameters through their active involvement in solving real-life problems.This game lands on the category of anti-phishing and malware as well[38].

Capture The Flag is an interactive puzzle game in the form of a competition in cybersecurity, known as Capture The Flag requires an individual to solve many different problems related to hacking. They include revealing messages, exploiting websites, and reverse engineering malicious software codes. To get the points, players search hidden in these challenges what are called flags. The game mechanics will foster research, practice and critical thinking in a time-based competitive scenario. It is well employed in the cyber realm among the security circles and in schools to hone skills[20].

Class CTF gets designed as an educational variant of classical ones. It provides tutorial and graded exercises designed to enable learners to develop baseline competencies in cybersecurity. The game is step-by-step, provides hints, and instant feedback, so it is simple in nature and can be played by those new to the world of cybersecurity. Our aim at taking this approach in increased difficulty levels is to make the players feel confident in themselves and generate solid knowledge around the basics of how malware and phishing work together with some simple exploits[11].

Hardware CTF targets the physical side of cybersecurity and brings real-world challenges of embedded devices, IoT systems, and hardware hacking. The goal is to find out a vulnerability inside a device that behaves similarly to an actual device by utilizing analysis of firmware, hardware debugging, and side-channel attacks inside the game. The game mechanism implies the contact with physical or emulated parts of hardware, encouraging the in-depth knowledge of how hardware layers could be used to attack the computer system instead of software exploits[49].

Control-Alt-Hack is an educational card game that instructs on cybersecurity with the use of realistic, mission-oriented scenarios. Players become ethical hackers employed by an imaginary company, resolving security issues with regards to phishing, malware, passwords, and insider attacks. By employing hacker profiles, mission cards, and action cards, players work together and strategize with respect to each mission with regards to the technological, ethical, and social aspects. The game's blend of humor, actual threats, and decision-making makes Control-Alt-Hack an engaging tool to learn the concepts of cybersecurity in an entertaining, experiential manner. This game falls under the ransomware category as well as phishing , password Protection and management category[8].

Gamifying Spoofing Defense

The Microsoft Elevation of Privilege (EoP) card game is a collaborative card game and it helps software developers and engineers to self-identify security vulnerabilities at the early design stage of a system. The game is played with a deck of cards that are placed in line with the STRIDE model of attacks namely: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. Each card has a potential threat and each card is read by the players together and discussed how each threat may be applicable to a certain system architecture. The team as a whole then improves the entire design in terms of security as they decide what are the dangers that might be in place and how these might gain entrance into the design. It will be a powerful, active way of instilling secure-by-design thinking and mindset, without code but still[28].

IoT-Poly is an educational game that teaches learners about IoT security in an experiential manner by presenting real-world attack scenarios. The learners participate in various exercises that relate to identifying vulnerabilities and decision-making with the intention of safeguarding IoT devices from attacks. The game evolves in difficulty as the course progresses, teaching learners to use cybersecurity principles through decision-making and problem-solving. Real-time feedback supports the learning process, and since IoT-Poly enables learners to practice IoT security in a real-world environment, the gap between theory and practice in IoT security knowledge is closed[33].

Network Nightmares is an educational tabletop game that instructs on network security by emula real-world network troubles such as ARP spoofing, VoIP issues, and packet anomalies. Teams of players diagnose and address these issues using tokens or cards to symbolize tools such as network taps and monitoring equipment. By experiencing the game in the form of scenarios, they examine network behavior, introduce countermeasures, and acquire practical methods for detecting and

mitigating security issues in an intuitive, collaborative fashion[9].

Gamification in Network Security

In CyberCIEGE, an individual plays the role of network administrators in securing information technology of a virtual firm. The game teaches basic security concepts as scenario-based practice in real-life attacks and dilemmas. The users build and secure networks via firewalls, VPNs, servers and formulate access control and encryption, carry out patching and physical security and train users on security policies. It has an integrated attack engine, which simulates attacks like Trojan, DoS, and insider attacks and puts the capacity of the user on the balancing act of security, user-friendliness, and budget when there is an increase in the stakes [3].

CyberNEXS is a cybersecurity simulation game in real-time that involves players to act as attackers or defenders in a virtual environment to perform in divisions within some networks. Defenders can include resources to defend high value targets, use firewalls, and react to continuous attacks and attackers can lay in wait to unleash their exploits. The game focuses on strategic game choices and resource management in stressful situations where a player must simulate realistic scenarios of cyber warfare and work collectively as a team, think quickly, and adjust. This game is also categorized as anti-phishing and malware[6].

ARP Adventure is a practical game based on scenarios that aim at educating the students on concepts related to network security particularly ARP spoofing and man in the middle attacks. The simulated network traffic is analyzed in real time, anomalies are detected by the players and defenses are used to preserve the integrity of the communication. Interactive network mapping and packet tracing programs are used in the game, which also means it is a resourceful demonstration of learning what network-level attacks and defense consists of. This game also comes into the network security training category[69].

Other

ConfigPlay project is a turn based strategic plays board game that trains on cybersecurity in the form of simulated attack and defended instances on computer networks. The objective of the game play is the utilization of scarce resources by the attackers or the defenders so as to exploit, or defend, network nodes like servers and firewalls. On the side of the defenders are the use of tools like firewall, IDS, and patches and on the other side are tactics like scanning, phishing, and malware. Making a choice at every turn, the success of the game preserves the management of risks and the acquisition or surrender of resources. The game in its interactive, non-classical way promotes understanding of the threat modeling, vulnerabilities, and defensive approaches in a way that is both more experiential and more accessible than conventional capabilities and competence-based learning. This game comes in categories of authentication Flaws, misconfigurations, race conditions, privilege Escalation, CVE-based vulnerability exploitation[24].

CyberAIMs is an educational simulation video game for learning adversary behavior

and cyber risk assessment. Players become either attackers or defenders, each of them have attributes such as resources, skills, and motivation. The game unfolds in time-segmented rounds (ticks), within which agents make strategic decisions—e.g., attack, defend, or invest in skills. Success is determined by probability calculations based on agent attributes. Attackers acquire and defenders lose resources when attacks are successful, mirroring real-life repercussions. Asset valuation and risk measures such as SLE and ALE are also included, allowing students to see how cyber behaviors affect finances. This game falls under user Behavior & decision-Making, cybersecurity awareness training, risk & resource management, privilege escalation & exploitation categories[29].

2.3 Key Findings of existing works

Despite high exposure to the digital world, the current level of cybersecurity awareness among students appears to be insufficient, as evidenced by several studies that highlight gaps in knowledge and lack of engagement with cybersecurity topics. A large portion of university students still lack basic cybersecurity awareness training, even in specialized fields like computer science (CS) and IT/cybersecurity.

- **Basic Cybersecurity awareness:** While there is some recognition of cybersecurity risks among students, many fail to implement proper security measures. For example, a study found that 68% of IT/cybersecurity students, 80% of CS students, and 72% of non-CS students downloaded files from untrusted sources, which exposes them to cyber risks [73]. Similarly, the habit of keeping software up to date was neglected by a significant number of students: 16% of CS students, 12% of IT students, and 8% of non-CS students using outdated softwares.

- **Weak Password Practices:** Password security is another major concern. The same study revealed that a large portion of students, regardless of their field of study, do not change their passwords frequently enough. Only 8% of non-CS students change their passwords weekly, and many students never or seldom change their passwords, increasing their vulnerability to cyber-attacks.

- **Online Behaviors:** The amount of time spent online also increases exposure to cybersecurity threats. For instance, 24% of IT students spend over 10 hours online per day, compared to 16% of CS students and 8% of non-CS students . Despite this high usage, many students neglect to adopt security measures such as using strong passwords or safeguarding personal information.

- **Perception of Cybersecurity Responsibility:** A troubling finding is that a portion of students, including CS students and non-CS students, believe cybersecurity is solely the concern of organizations, not individuals. This attitude indicates a lack of personal accountability in ensuring their own digital safety.

Overall, university students display a concerning lack of cybersecurity awareness, which leaves them vulnerable to a wide range of digital threats, including phishing,

malware, identity theft and so on. While this issue is more severe for non-CS students, even those studying in related fields like IT and cybersecurity are not immune to these lapses in security habits. This highlights the need for more comprehensive, mandatory cybersecurity training within the education system to improve students' online safety practices.

Traditional methods of teaching, such as text-based training and generic educational programs, have been criticized for their lack of engagement and inability to effectively address the complexities of cybersecurity. While some students possess basic awareness, many struggle with understanding and retaining key cybersecurity concepts, especially when taught using conventional methods. Gamified learning methods outperform traditional approaches in acquiring student engagement, promoting deeper learning, better retention, and increased motivation for a complex subject like cybersecurity. Table 2.1 highlights the key differences between Gamified and Non-Gamified Methods.

Aspect	**Gamified Methods**	**Non-Gamified Methods**
Engagement	Interactive and engaging, with real-life challenges and feedback [25], [63].	Static and text-based, leading to less active participation [25].
Learning Outcomes	Higher test scores and better understanding of concepts [25], [50].	Lower improvement in test scores and concept retention [50].
Knowledge Retention	Learning from failures improves long-term retention [58], [63].	Emphasis on theoretical knowledge; lower retention [58].
Motivation and Confidence	Contextualized learning boosts confidence and motivation [50].	Limited opportunities to build confidence [50].
Satisfaction	Fun and engaging but may receive slightly lower satisfaction scores [25].	Familiar methods sometimes rated higher in satisfaction [25].
Behavioral Impact	Improves practical behaviors like cybersecurity awareness and application of best practices [58].	Limited impact on real-world behavioral changes [58].

Table 2.1: Comparison of Gamified and Non-Gamified Methods

Several gamification strategies have been identified as effective in improving cybersecurity awareness among university students. These strategies utilize interactive, engaging, and immersive learning tools that simulate real-world cybersecurity scenarios. Here are a few key takeaways-

- Instant Feedback and Motivation: Features like leaderboards, scoring, and feedback help motivate students and provide immediate reinforcement, leading to more effective learning and improved behavior.
- Practical Learning tool: Many gamification strategies simulate real-life cybersecurity challenges, allowing students to practice skills such as identifying phishing attempts, protecting data, and responding to cyber threats in controlled environments. A study on scenario-based eLearning suggests such gamified

approach introduces active learning strategies such as problem-based or case-based learning by using interactive scenarios [32].

- Creating Interactive Scenarios: Gamified tools, such as role-playing, CTF games, and serious games, make cybersecurity education more engaging and enjoyable using interactive scenarios, which helps students better retain information and apply it in real-world scenarios.

For our research, we decided to make a scenario-based visual novel game as it creates an interactive and engaging learning environment where students can actively participate, face challenges, and receive real-time feedback. This engagement encourages students to learn from both successes and failures, making the learning process more dynamic and motivating compared to the passive nature of traditional, literature-based teaching methods. There are other gamification approaches like- RPG,CTF, Serious games, Simulation based games; all with their own niche benefits and applications. Our findings suggest that gamification offers a more dynamic, effective, and enjoyable alternative to traditional methods of education.

As cybersecurity threats continue to evolve in complexity and scale, gamified training seeks to improve user engagement, motivation, and ultimately, competence. Applying these game design elements to a learning environment transforms abstract concepts and technical knowledge into interactive, immersive, and often competitive experiences. Here are some of the learning goals that gamification aims to achieve-

- The primary learning goal targeted by gamification strategies in cybersecurity education is **enhancing users' ability to recognize and prevent cyber threats**. Several games, such as Anti-Phishing Phil and Phishy, focus on teaching players how to identify phishing URLs and suspicious links by familiarizing them with common phishing indicators like misspelled domains or deceptive subdomains [4], [23]. Similarly, games like Persuaded and Secu-One train users to detect social engineering attacks and respond appropriately to phishing attempts, emphasizing the importance of vigilance against such manipulations [22], [34]. Other games also incorporate learning objectives around recognizing malware, ransomware, and network-based attacks such as spoofing and ARP poisoning, expanding the learner's awareness of diverse cyber threats [8], [9], [28].

- Another important goal is to develop **decision-making and risk management skills**. Games such as Cyber Smart and CyberNEXS engage players in making timely decisions under pressure, balancing resource allocation, and managing defenses like firewalls and patches to protect virtual assets [6], [79]. These games simulate real-world dilemmas where players must weigh security against usability or budget constraints, cultivating strategic thinking that reflects practical cybersecurity challenges [3], [12]. This goal also encompasses training users to understand the consequences of their security choices, fostering a mindset geared towards proactive risk mitigation.

- Gamification further aims to **improve security behaviors and overall cybersecurity awareness** among users. Through interactive formats and immediate feedback, games encourage players to adopt safer online habits such

as creating strong passwords, avoiding suspicious downloads, and maintaining skepticism toward unsolicited communications [7], [41]. Experiential games like IoT-Poly and Network Nightmares highlight the significance of secure design principles and defensive measures, helping players internalize secure-by-design thinking and best practices for protecting interconnected devices and networks [9], [33].

- In addition to awareness and decision-making, many games target **hands-on technical skills and problem-solving abilities** . Competitive puzzle games like Capture The Flag and its educational variants provide learners with opportunities to practice decoding messages, reverse engineering malware, and exploiting vulnerabilities in a controlled environment[11], [20]. Others, such as Hardware CTF, focus on the physical and embedded aspects of cybersecurity, teaching players about hardware-level attacks and defenses, thereby broadening their technical competence beyond software-centric threats [49]. These activities promote active engagement and deeper understanding through practical challenges.

- **Collaboration and communication skills** are also nurtured in multiplayer or team-based cybersecurity games. For example, Security Empire and Network Nightmares encourage players to coordinate responses, share information, and strategize collectively to fend off attacks, emphasizing that cybersecurity is often a shared responsibility requiring effective teamwork [9], [12]. Such social interaction in game settings strengthens communication and collective problem-solving, essential skills in real-world security operations.

In summary, gamification strategies in cybersecurity education primarily target learning goals that improve threat recognition, decision-making under risk, secure behavior adoption,technical skills, collaborative competence etc. These multifaceted objectives contribute to building a well-rounded cybersecurity skill set suited to the evolving complexities of modern digital environments.

Understanding how the audience perceive gamification is crucial to designing effective and inclusive educational tools, particularly in complex domains like cybersecurity. Here are some key takeaways-

- The general perception towards gamification in cybersecurity education is generally positive, with learners showing increased **engagement, motivation, and interest** in learning complex topics. Many of the reviewed games prioritize interactivity and narrative immersion, which learners find more enjoyable compared to traditional instructional methods. For instance, Anti-Phishing Phil and Phishy employ animated characters, levels, and immediate feedback to teach phishing detection—strategies that have been shown to keep players engaged and encouraged repeated play, ultimately reinforcing learning[4], [23].

- Gamified environments are particularly appreciated for their ability to **reduce the cognitive load of learning technical content** by embedding knowledge into game play. In Hacked Time and Internet Hero, for example, users praised the narrative-based format and the point-and-click mechanics for making cybersecurity scenarios feel accessible and relatable. These story-driven

designs allow players to explore consequences of actions in a safe space, which learners perceived as empowering and less intimidating than formal testing [7], [41].

- Moreover, competitive and cooperative elements **enhance motivation and performance** . In multiplayer games like Security Empire and CyberNEXS, participants respond positively to the team-based dynamics and resource management challenges, which mirror real-world scenarios. Such competitive strategy games are perceived as stimulating and realistic, providing a sense of urgency and relevance that drives sustained participation and deeper understanding [6].
- **Personalized learning and feedback**, as seen in Internet Hero and SecuOne, are also highly valued by users. These features help learners track their own progress and identify areas for improvement, increasing their confidence and sense of ownership over their learning. Adaptive difficulty and real-time feedback were cited as helpful in sustaining interest, especially for learners with varying levels of cybersecurity knowledge [34].

Overall, gamification receives a favorable perception from a learner's perspective. Users find gamified cybersecurity training more engaging, motivating, and effective than passive methods, especially when the games are immersive, narrative-rich, and aligned with real-world scenarios..

2.4 Our Work

In existing works we have mentioned different kind of games which were developed to enhance cybersecurity awareness. Most of the games target specific threats like phishing, password management or malware. For an example, games like Anti-Phising Phill and Phishy were solely focused on Phishing. On the other hand Hacked Time and Internet Hero focuses upon enhancing password practices by interactive story telling. These approaches are effective in their own scope. However, they do not cover the wide range of threats which students could face in their day to day life.

Furthermore, most of the games were made for office workers, enterprise users or for computer science students of a developing country. This makes them a little bit less suitable for non-technical students in Bangladesh who often lacks the knowledge but very much active in online. Also, some of the games uses card mechanics, puzzle formats or capture the flag (CTF). Which might be a little bit boring for the students.

Our game tries to fill the gaps, it covers seven major threats which are : password protection, ransomware, identity theft, phishing, malware, malicious pop up ads and cryptojacking in a single game. Instead of the existing type of game we created a story based visual novel game where player need to make critical decisions and based on their decisions the story will progress. In the game there were instant feedback after every occurrence. Also we added quizzes,scoring system and leader board system to grab the attention of the participants.

Table 2.2 shows the comparison between our game and the existing game:

Aspect	Existing Games	Our Game (Visual Novel)
Scope of Threats	Most games focus on a single or limited threat such as phishing (Anti-Phishing Phil, Phishy) or password security (Hacked Time) [4][23][41].	Covers **seven threats**: Passwords, Ransomware, Identity Theft, Phishing, Malware, Pop-up Ads, Cryptojacking.
Target Audience	Designed mainly for enterprise users or CS/IT students in developed countries [7][23].	Specifically designed for **non-CS university students in Bangladesh**, who are highly vulnerable and underrepresented.
Game Format	Puzzle games, card games, Capture-the-Flag, or quiz-based training. Very few visual novel story-driven games [8][20][22][66][90].	**Story-driven visual novel** format with interactive dialogues and branching decisions.
Learning Approach	Focuses on recognition tasks (e.g., spotting phishing URLs) or abstract simulations [4][23][36].	Uses **constructivist learning theory**, with real-world inspired stories and analogies tailored to local student context.
Gamification Elements	Some provide feedback or scoring; often limited replay value [4][23][41].	**Instant feedback, quizzes, scoring system, and leaderboards** encourage replay and sustained engagement.
Cultural Relevance	Mostly Western-centric scenarios, not adapted to local behavior [7][23][79].	Localized for **Bangladeshi students' online habits**, addressing unsafe downloads, weak passwords, pop-ups, etc.

Table 2.2: Comparison of Existing Gamified Cybersecurity Games vs. Our Proposed Game

Chapter 3

Methodology

A clear and organized plan is important when using strategies, methods, and steps in the study. This helps to set up the process of the research and also ensures that all the research questions and objectives are properly handled. It also helps to maintain a consistent flow for developing the research. The workflow shown in Figure 3.1 outlines how the research will be carried out. The workflow gives a clear path to follow, and it ensures that the research has been done properly in a way which guides us to dependable results.

3.1 Methodology Flow-diagram

In Pre-Thesis 1 We decided to make a visual novel game to provide various scenarios, each symbolizing various cyber threats and give the players multiple options to continue conversation to figure out the nature of the problem and ultimately ending up on a decision based on their choice. Based on the opinions of security experts [19] we have created the story for our game and started developing the game Pre-Thesis 2. The story we created were based on the following principles-

- Use of analogies to make the scenarios easier to relate to for the students
- Use of real stories using fictional characters and scenarios to describe security events and consequences of security breaches
- Describe the information in a way that people understand and can visualize.

By following these things we have successfully completed developing the game. After that we created a text based tutorial from the existing material. We conducted the evaluation on two different groups. Both groups faced a set of questionnaires before playing the game or reading the tutorial. The **control group** had read the tutorial, and the experimental group had played the game after the pre-interview questions. After the participant finished reading the material or playing the game, they faced another set of questionnaires that were not exactly similar to the previous questionnaire but a little bit different. Then we compared and analyzed the results of both groups.

Here is the flowchart (Figure 3.1) that illustrates the workflow for accomplishing our research objectives-

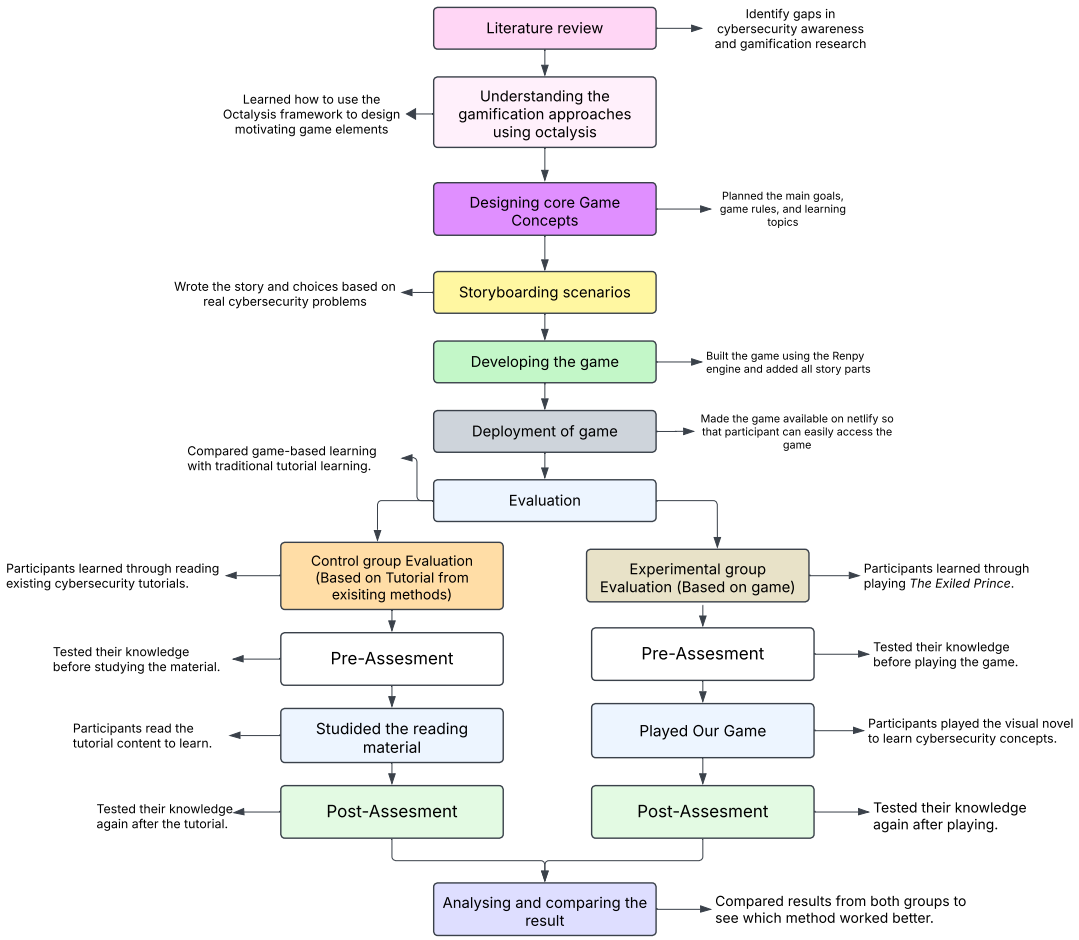

Figure 3.1: Workflow.

3.2 Understanding the Gamification Approaches Using Octalysis Framework

The Octalysis Framework was developed by Yu-kai Chou [92]. It is a comprehensive model for analyzing and designing gamified experiences. It identifies eight core drives of human motivation that influence engagement and behavior:

1. **Epic Meaning & Calling**: Feeling part of something bigger than oneself; a purpose beyond personal gain.
2. **Development & Accomplishment**: Progress, mastery, achievement, and measurable success.
3. **Empowerment of Creativity & Feedback**: Freedom to explore, experiment, and receive immediate feedback on choices.

4. **Ownership & Possession**: Desire to collect, upgrade, and control resources or in-game assets.
5. **Social Influence & Relatedness**: Motivation through social connections, competition, recognition, or collaboration.
6. **Scarcity & Impatience**: Wanting something rare, locked, or available only for a limited time.
7. **Unpredictability & Curiosity**: Mystery, surprises, and the excitement of discovering unknown outcomes.
8. **Loss & Avoidance**: Fear of losing something valuable or missing out on opportunities.

Our game was designed in a way so that it could fulfill the octalysis framework as much as it can. We have added a leaderboard system, progression, instant feedback, unexpected events, epic meanings by the prince who was tasked to rebuild the kingdom, hidden messages and many more.

3.3 Targeted Demographics

The growth of technology has been increasing at a high rate over recent years. Different types of people are continuously engaging with the online world. However, the online world can also present serious risks if proper security awareness is not established. A review of various studies, both global and local, reveals that many people, particularly in Bangladesh, lack the necessary knowledge of how to protect themselves from the risky online world. Even though university students have knowledge about the online world, they often lack the understanding of how to protect themselves, which makes them more vulnerable to security threats. However, university students from computer science backgrounds, in most cases, have better knowledge of cybersecurity than non-computer science students. Given the large number of non-computer science university students in Bangladesh, it raises the question of whether they have proper knowledge about cybersecurity to protect themselves from cyber threats. This has driven our decision to focus on Bangladeshi university students from non-computer science backgrounds for the research.

3.4 Design and Development

We have designed a visual novel game for non-technical university students. The game is very simple and straightforward. In the game the player will go through different kinds of scenarios and will learn about the cybersecurity issues which we had worked on. The game is easy as well as interesting. To make it competitive we have added a quiz point system and leaderboard. So, the user feels that they can play the game in a more focused way and score more and more so that the player is the number one in the leaderboard. Also we have added instant feedback.

So that the players get feedback about their action. To make the game interesting there were several tasks like building five pillars correctly, identifying real armor and fake armor. As the existing materials are complicated and monotonous for non-technical background students we have tried to make our game easy and simple as well as interesting. Even Though our main users were university students from non-technical backgrounds, the layout and content of The Exiled Prince are non-complex and interactive so that any non-cs or non-technical person can play the game and learn from it. The aim was for the cybersecurity education of the game to extend further than just from academia.

3.4.1 Why a Visual Novel Game?

Given the current landscape of cybersecurity education among university students, the need for a more engaging and impactful learning method is undeniable. Various research consistently shows that many students exhibit significant gaps in both cybersecurity knowledge and behavior. For example, despite being immersed in the digital world, many students still engage in risky practices like downloading from untrusted sources or neglecting software updates[18]. Even more concerning is the tendency of students to shift cybersecurity responsibility to institutions rather than seeing it as a personal duty. Traditional methods of cybersecurity instruction have largely failed to address these issues due to their text-heavy, passive nature, which often leads to low engagement and poor knowledge retention. Recent studies showed that story based gamified approaches are more efficient in grabbing attention of the users. Scholefield and Shepherd [35] showed that role playing games (RPG) on password security have a major effect in enhancing the knowledge of users. Also, Sharif and Ameen [51] and Fatokun et al. [60], talked about gamification which increases the motivation, awareness and behavioral change toward safer online habits. This work shows us that learning from interactive storytelling not only improves the knowledge but also grabs the attention of the users.

The visual novel type games specifically align with these findings because visual novel games merge decision making as well as story telling. This allows the users to experience real world cyber threats through the storyline [87]. So based on all these, we can tell that adopting a visual novel style game gives us an accessible as well as human-centered approach which combines both storytelling interaction and reflection. This thing not only enhances the knowledge but also lets the users enjoy the process.

3.4.2 Designing Core Game Concept

Our game, The Exiled Prince was designed by combining interactive gameplay with cybersecurity education. The main gameplay mechanisms include exploration, decision-making, choosing the correct options and actively participating in quizzes. The game was designed to align with both game progression and educational goals ensuring that players remain engaged while learning important concepts. Players are required to analyze different scenarios and make appropriate decisions based on the situations they encounter. To motivate and reward players the game includes

features such as unlocking hidden messages earning points after completing quizzes and storing their names in a leaderboard. The game also provides instant feedback which allows players to understand mistakes and learn from them immediately. All these core concepts were carefully designed to educate users in an enjoyable and interactive way, combining challenge, learning and fun seamlessly. By integrating gameplay with learning, the game encourages players to think critically, make informed decisions and actively engage with cybersecurity concepts throughout their journey.

3.4.3 Storyboarding Scenarios

This part involves planning the sequence of events, player interactions and decision points within the game. Each scenario represents a specific cybersecurity threat and since there were seven threats in total we had to carefully connect the story with each scenario to ensure a smooth and logical progression. Key elements such as characters, dialogues and actions were outlined in a written format which allowed us to anticipate the different paths a player might take. By mapping all the scenarios to particular threats we ensured that the narrative, gameplay mechanics and learning objectives were fully aligned. Story boarding also helped identify critical learning moments making it easier to integrate educational content naturally into each scenario. This process not only guided game development but also ensured that players would experience the story and learn in a coherent and engaging way. The full story, including all scenarios and their underlying meanings is detailed in the following chapter.

3.4.4 Developing the Game

The game was developed using different principles. Two major principles were constructive hearing principle and Human Centered Design principles.

Constructive Learning Principle

Development of the game is done by using the Constructivist Learning Theory. This principle helps the learners to actively create their own understanding from experiences as well as reflection [1][2]. Players will learn from engaging with scenarios, by making decisions and by observing all the consequences of their actions rather than the old -fashioned way which is just receiving the information. Each chapter is designed to make students entertain as well as to learn realistic metaphors of complex cyber security threats. Not only that, students can apply critical thinking to resolve them as well. For example, denying to give armor to the suspicious person by correctly observing the difference between real and the fake ones corresponds to recognizing a phishing website. Also while collecting evidences from the underground market simulates the network defense as well as threat investigation This experiential learning format was also used for learning practices utilized by a serious game named Riskio, which is also built on the constructive principles. By following the constructive learning prince principle Riskio game improved participants

understanding of cyber threats by the decision consequences as well as role-play [42]. As well as, studies on scenario-based eLearing confirm that learners really perform well under an interactive and narrative-driven challengers [31]. So by visualizing the digital threats through narratives and fictional yet relatable environments, the game will help the students to learn the essential knowledge about security threats as well as it will encourage them to apply the cybersecurity practices. Which will be a long-term behavioral change.

Application of Human-Centered Design (HCD) Principles in Our Game (The Exiled Prince)

Our game, The Exiled Prince was designed using the Human-Centered Design as defined by NIST [57]. The design process therefore centered on user understanding, engagement with users over development, and ongoing iteration based on feedback so as to make the game not only educational but also enjoyable. The following points describe how the game aligns with the key principles of the Human-Centered Design (HCD) approach.

The Design Was Based on Understanding Users, Tasks, and Environments

The game design started with familiarizing with target users which are Bangladeshi university students. Based on the literature review and context analysis, we recognized their weak cybersecurity awareness, online activity, and virtual learning atmosphere. These defines framed their needs, motivation, and learning barriers and gave us the idea for designing contents that would match with their acquaintance with familiarity and cultural background.

Users Were Involved Throughout Design and Development

Our target audience was students with non-technical backgrounds. So the students were also involved in the process of user studies. They played the game, provided feedback and were part of discussions of usability and engagement. Their feedback allowed us to determine what would be the best for learning from different parts of the game and what needed to be changed which ensures that the users also had a part throughout the design process.

The Design Was Driven and Refined by User-Centered Evaluation

We performed side by side evaluations of The Exiled Prince compared with a conventional text based tutorial. The results from pre and post-interviews and from the user allowed us to measure the learning outcome as well as usage levels. From this information, we improved the game mechanisms, story flow and instructions to make the game more user friendly and effective.

The Process was Iterative

The game design process itself wasn't a one step creation. It was an iterative process. In the initial stage development, the game was tested with the users and feedback was collected and improvements were made based on the feedback of the user. This ongoing process of testing and revising helped us to improve usability, learning quality and motivation of the player in the long run.

The design addresses the whole user experience

We aimed at developing an entertaining and non-technical learning experience instead of a technical one. The game was simple, pleasant on the eyes, and non-specialized in terms of language used. The use of interactive storytelling, branches, and questions turned out the gameplay both educative and fun for non-technical students.

The design team includes multi-disciplinary skills and perspectives

We designed from scratch and combined knowledge of computer science, cybersecurity, storytelling and education on cybersecurity. This thing ensured that technical and complicated aspects of cybersecurity were accurately represented by our game while maintaining the strong narrative as well as learning elements which caught the attention of the students who are from diverse backgrounds.

Table 3.1 is the summary of how our game applied the human-centered design (HCD) principles.

HCD Principle	**Application in the Game**
The design is based on understanding users, tasks, and environments	We studied Bangladeshi university students, their low cybersecurity awareness, and online learning habits to design content suited to their needs and culture.
Users are involved throughout design and development	Students participated in play testing, provided feedback, and helped identify improvements, ensuring user involvement throughout development.
The design is driven and refined by user-centered evaluation	We compared the game with a traditional tutorial using pre- and post-assessments, then refined gameplay, story flow, and instructions based on feedback.
The process is iterative	The game went through multiple testing and improvement cycles, where user feedback guided refinements to usability, learning quality, and engagement.
The design addresses the whole user experience	We focused on creating a simple, engaging, and visually appealing game using interactive storytelling and quizzes to make learning enjoyable for non-technical users.
The design team includes multi-disciplinary skills and perspectives	Our team combined expertise in computer science, cybersecurity, storytelling, and education to ensure both technical accuracy and an effective learning experience.

Table 3.1: Application of Human-Centered Design (HCD) Principles in *The Exiled Prince*

3.4.5 Deployment of the Game

We wanted to make the game easily accessible. Because of this reason we hosted it on a web based platform. This helped the participants to access the game easily. Also the users could access our game with any kind of device as it was web based. All they needed was a device and the internet. If they had these two things they could easily play as well as enjoy the game. By hosting the game in an online platform we ensured the easy accessibility for all the users and fulfilled our prior target.

3.5 Evaluation

To assess the effectiveness of our game we conducted a controlled study. We have compared the game with a tutorial which was made out of existing text based material. The evaluation system gave us the idea about participants' prior knowledge, their engagement during the activity as well as their ability to apply the cybersecurity concepts in realistic solutions before and after playing games or reading the tutorial. We measured the learning outcomes through pre and post interview questionnaires. Additionally we collected qualitative feedback on user experience, preferences and usefulness of the game versus the traditional tutorial.

3.5.1 Participant Requirement

We have selected participants from different universities and also from different departments which have less engagement with the cybersecurity topics. Firstly we have asked three screening questions. If we get No for all the screening questions then we proceed with the participant.

3.5.2 Controlled Study

To assess the game we conducted a controlled study. There were two groups in our study. Both groups had equal number of participants and the groups are:

1. Control Group: After conducting the pre-interview we provided the printed copy of the tutorial to the control group for reading. We recorded the time that required to complete the tutorial.
2. Experimental Group: Just like the control group we provided the link of our game to the experimental group for playing the game. We recorded the time for the experimental group to finish the game as well.

Ethical Consideration

Before conducting the evaluation process we have taken consent from each and every participant. The consent was taken in a form where they signed. One copy of the consent were given to the participant and we kept one copy.

Pre-Assessment

We have conducted two interviews. The pre-interview was a structured interview. This allowed us to assess their baseline understanding before moving on to the game or tutorial.

Interaction with the Game or Studying the Tutorial

After the pre-assessment we let the participants interact with the game or study the tutorial. As mentioned before the control group studied the tutorial and the experiment interacted with the game. During the process we were present with the participants so that if they face any kind of problem we could help them. Furthermore, we also measured the time that was needed to play the game as well as reading the tutorial. After successfully interacting with the game or reading the tutorial we conducted another assessment.

Post-assessment

In the post-interview questionnaire we designed the questions so that participants needed to provide detailed answers. This interview helped us to assess the enhancement or reduction in knowledge after reading the tutorial or playing the game.

Outcome and Evaluation

After conducting the both pre and post assessment the answers were evaluated by a single evaluator person to avoid any kind of inconsistency. After successfully evaluating all the participants we conducted different kinds of statistical tests to find the outcomes.

3.6 Analysis and Comparing the Result

After successfully evaluating the result we have started data analyzing. We developed three hypotheses and started to test them. The process and result of the hypothesis testing will be found in the following chapter.

3.7 Summary

This chapter provided a clear and concise overview of our research methodology. Which included planning the study as well as developing a visual novel game, evaluating the outcome and conducting statistical tests which will be discussed in the following chapters.

Chapter 4

A Gamified Solution: The Exiled Prince

We have developed a visual novel game. The visual novel game is named **The Exiled Prince**. Our visual novel game has been designed to simulate the cybersecurity challenges by using metaphorical storytelling rather than the traditional ways. The full structure and functionality of the visual novel game and details about the game will be defined here.

4.1 Game Development Stack

The platform we choose to design the game is **Renpy** [86]. Renpy is a Python-script based visual novel engine which was developed to create interactive story games that can run directly in a web browser as well as in Windows, Linux, Android and iOS. It is an open source and lightweight game engine. Because of this reason it is easy to customize and extend. Renpy also supports multimedia elements like pictures, audio and animations. It also provides a simple scripting sentence which allows the developers to define scenes, characters, choices and branching paths without complex coding. As browser based deployment is possible in Renpy, this depicts games can be played on almost any device that do not need any kind of installation. This is the reason which makes it not only an accessible but also a flexible option.

4.2 Game Components

The game is being designed with different kinds of narratives, branching of choices as well as real time decision feedback which simulates the cybersecurity threats. We have used different 2D anime-style graphics and different types of eye pleasing backgrounds to provide an enhanced experience for the players. The background includes various places such as markets, kingdom and many more. There are a total 3 chapters in our visual novel games and each chapter defines different types of security threats. Some of the characters and scenarios are shown in the picture down below:

Figure 4.1: Prince

Figure 4.2: Advisor

Figure 4.3: Suspicious Character

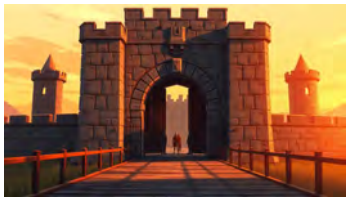

Figure 4.4: Background Scenario 1

Figure 4.5: Background Scenario 2

Figure 4.6: Background Scenario 3

Characters:

- Prince : The prince is the central protagonist. The story revolves around the prince. Figure 4.1 is the demonstration of the sprite that we used in our visual novel game as prince.
- Advisor: The advisor is the one who helps the prince in different situations. Figure 4.2 is the demonstration of the sprite that we used in our visual novel game as advisor.
- Builder, Military, Digging leaders : These characters represent key roles to rebuild the kingdom
- Suspicious Character: The suspicious character is a threat for the kingdom who tries to scam. This character tries to fulfill a special kind of task. Figure 4.3 is the demonstration of the sprite that we used in our visual novel game as a specious character.
- Witch: Witch has been shown as an antagonist in our visual novel. This character can be considered as a villain in the story.
- Vendors: The vendors have been introduced in this story to represent the threats like malware, cryptojacking and malicious pop up ads.
- Villagers, guards, blacksmith: These characters are the support role in the story and they help the player to uncover as well as enhance the experience of the game.

Secene setup: The player explores different kinds of scenarios and things while playing the game. Each and every scenario has been used as different kinds of narratives. Things like abandoned kingdom, dark markets, hidden passageways all have different kinds of meanings. Figure 4.4, Figure 4.5, Figure 4.6 are some of the scenes that have been used in our game.

UI Elements: Dialogue boxes with multiple choices are present in the game. Also the numerical system has been used to represent the **"Five Pillars of Defence"** which is for password protection. Also different kinds of ui elements were used in the game.

4.3 Game Deployment and Hosting on Netlify

The game is hosted on a cloud-based platform called **Netlify** [94]. It is very simple for developers to host and deploy web applications. Because it provides free hosting, automatic SSL, and quick worldwide delivery through its Content Delivery Network (CDN), it is perfect for static websites and browser-based games like visual novels. Netlify does not require a server-side GPU or CPU for players because the game is played in the user's web browser. Browser-based games are compatible with the majority of contemporary computers, laptops, and even smartphones; players only need a device with a modern web browser and a moderate amount of processing power. All you need to play the game is a browser and an internet connection.

The game can be accessed at the following link: https://exile-prince.netlify.app/

Requirement for playing the game:

- Modern web browser (Chrome, Firefox, Edge, Safari)
- Internet connection
- No dedicated GPU needed; CPU of a standard modern device is sufficient
- Works on desktops, laptops, and mobile devices

4.4 Game Story

The narrative of the game is divided into major chapters. There are three chapters in the game. In the beginning from the past history the player gets the idea about ransomware and why the kingdom was destroyed. Then chapter 1 represents password protection. Chapter 2 represents identity theft, phishing. Chapter 3 represents malware, cryptojacking and malicious pop-up ads. In the game the player plays as the prince throughout the entire story.

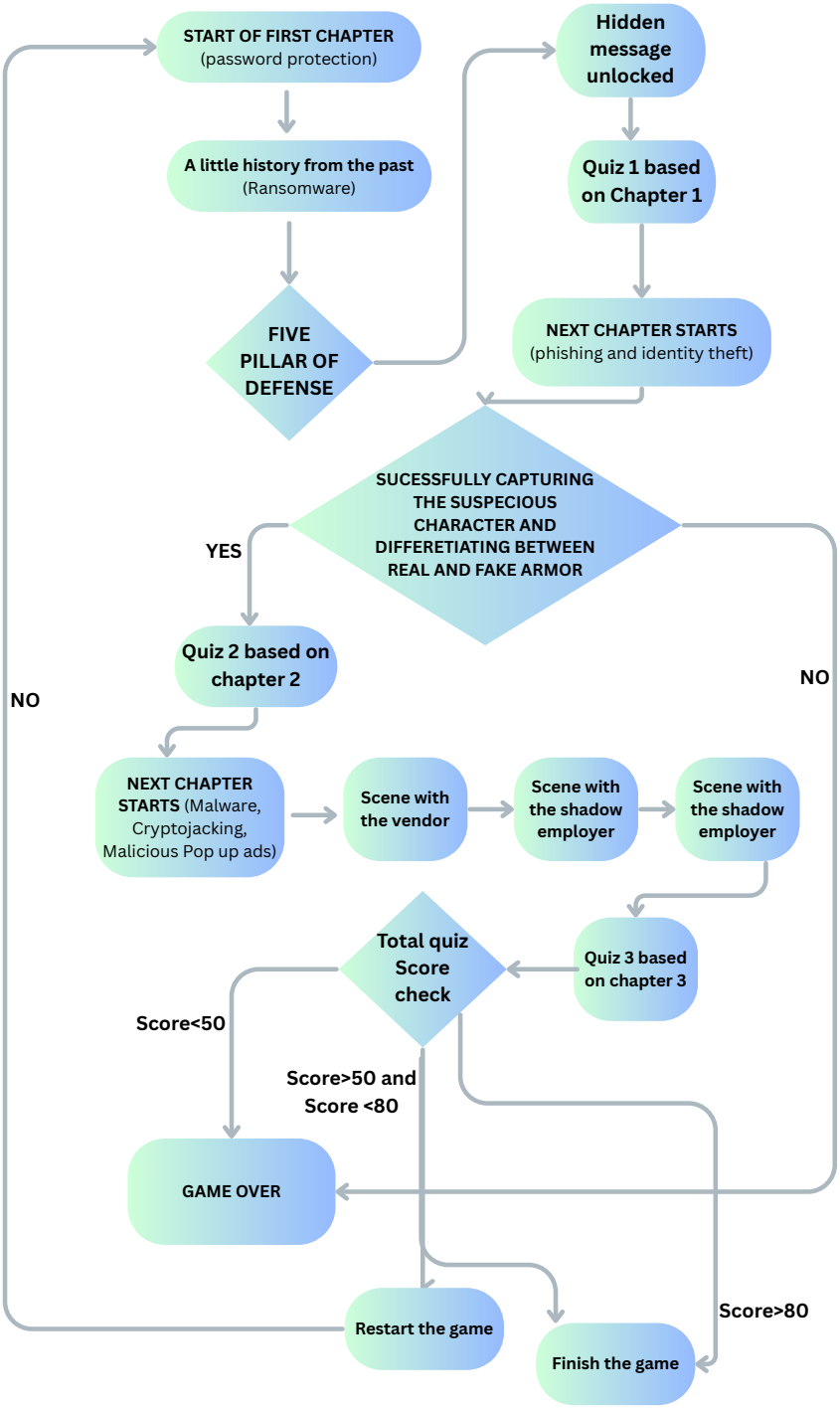

Figure 4.7: Game story

Figure 4.7 shows the basic flow diagram of our game.

4.5 Story breakdown

The game begins with asking the players whether they have played any kind of visual games or not. If they select no then they will get the instructions about how

visual novel games work and what to do. If the player selects yes then they will be redirected into the game. The story of the game begins with some background about what happened to the kingdom and who did it. After the player gets to learn a little story from the past how the kingdom got destroyed by a witch.

Figure 4.8: Scenario 1

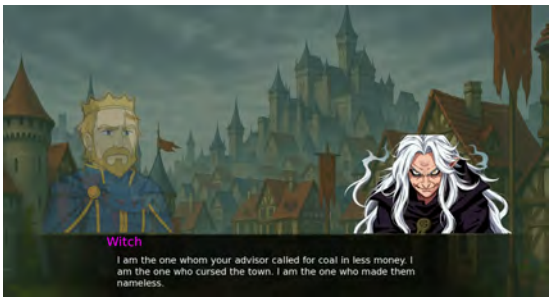

Figure 4.9: Scenario 2

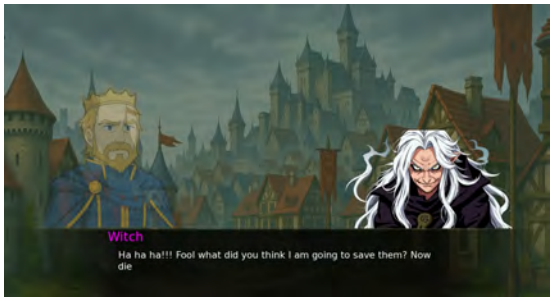

Figure 4.10: Scenario 3

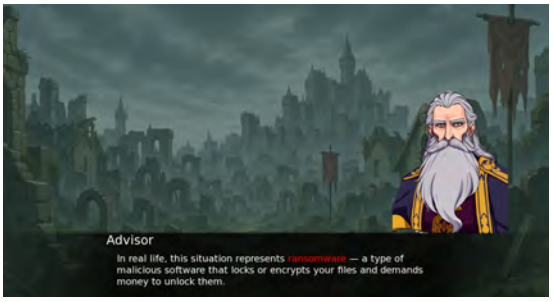

Figure 4.11: Scenario 4

This scenario where the kingdom get destroyed by the witch depicts **ransomware**. The scene begins with the advisor saying the kingdom is running low on coal. But an unknown neighboring kingdom is offering coal at a very low price. The king left the responsibility to the advisor and went for a tour regarding fix the problem that had arisen. After coming back to the kingdom the king found out it was a trap and a witch made every person nameless and asked ransom from the king to make things normal once again. The player will get the option to pay ransom or not pay ransom. But no matter what the player selects the witch will not restore anything and eventually the witch will kill the father of the prince. Figure 4.8 , Figure 4.9, Figure 4.10 and Figure 4.11 are some of the scenarios about ransomware from the game that the players face while playing. After that the game jumps into the main story. In down below the story of the each chapter will be described in details:

4.5.1 Chapter 1: Password Protection

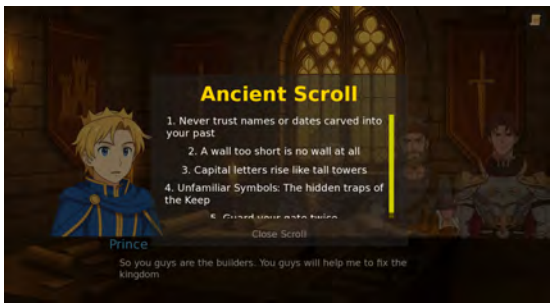

Figure 4.12: Scenario 5

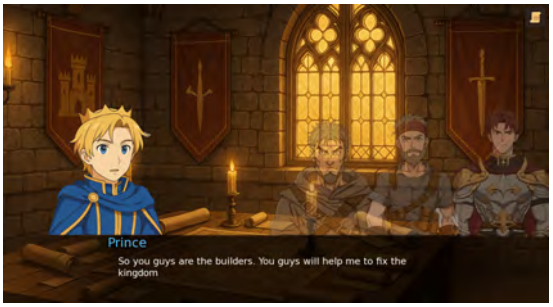

Figure 4.13: Scenario 6

Figure 4.14: Scenario 7

Figure 4.15: Scenario 8

Figure 4.16: Scenario 9

Chapter 1 is all about **password protection**. The prince finds a broken kingdom with a broken wall. Which leaves the kingdom open for all kind of attacks. The prince need to recreate the protective wall of the kingdom which was named as the Five pillars of the kingdom. This depicts the things that need to be followed while creating a password. We know there are several things that need to be considered while creating a password. The prince will meet with three builders and will order them to create different things. Each builder creates different kinds of things. The rules that need to be followed while creating a stronger wall will be found on a scroll which will appear during the meeting with the three builders. The content inside the scroll is shown in Figure 4.12. If the player chooses the correct thing then the scroll will be updated with secret messages. The secret messages depict how those tasks make the wall stronger. Also the advisor will tell why choosing the task was important and that particular task depicts the rule of password protection. After

successfully selecting 5 correct tasks a hidden message will appear on the scroll. And the player will be able to proceed to the next chapter. But if the player chooses one wrong task then the scroll will not be updated and in the end the player will be forced to give up which will make the player to play the game again from the part where the prince meets with the builders. Figure 4.13 , Figure 4.14, Figure 4.15 and Figure 4.16 are some of the scenarios about password protection from the game that the players face while playing.

4.5.2 Chapter 2: Identity Theft and Phishing

Figure 4.17: Scenario 10

Figure 4.18: Scenario 11

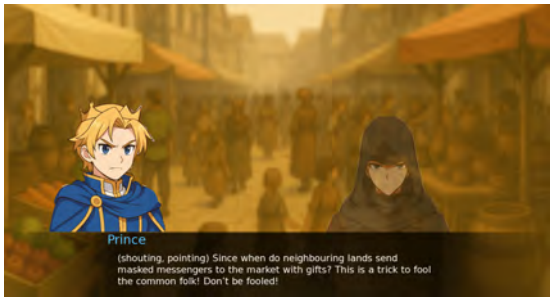

Figure 4.19: Scenario 12

The second chapter begins with a suspicious character claiming to be a messenger from a neighboring kingdom. He said the neighboring prince is offering free gold. But if someone wants to get free gold then the person must share their household mark and family name in order to get the free gold. This scene depicts online **identity theft**. In real life scammers often try to steal personal credentials by offering tempting rewards or free gifts [89]. Here players need to make a decision by selecting an option (Figure 4.18). The story will proceed based on the choice of the player. Figure 4.17, Figure 4.18 and Figure 4.19 are some of the scenarios about identity theft from the game that the players face while playing.

Figure 4.20: Scenario 13

Figure 4.21: Scenario 14

Figure 4.22: Scenario 15

Figure 4.23: Scenario 16

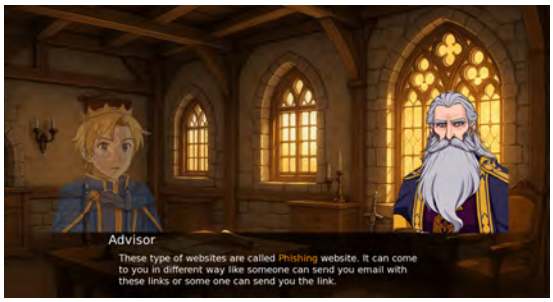

Figure 4.24: Scenario 17

After that in the same chapter the suspicious character will come back with a bit of a change in his appearance and then he will follow the guard and make an armor similar to the guard's armor. After that he will go to the blacksmith to change the armor with a real one by saying his armor is broken. Now the player will have the task to differentiate between the real armor and the fake armor (Figure 4.22). This scene depicts **phishing**. In phishing attacks there is minimal change between a real website and a fake website or between a real email or fake email [40]. If the player successfully differentiates between the armors and chooses the correct option then the story will progress otherwise the game will be over and the player will have to play the game from the beginning of chapter 2. Figure 4.20, Figure 4.21, Figure 4.22, Figure 4.23, Figure 4.24 are some of the scenarios about phishing from the game that the players face while playing.

4.5.3 Chapter 3: Malware, Cryptojacking and Malicious Pop-Up Ads

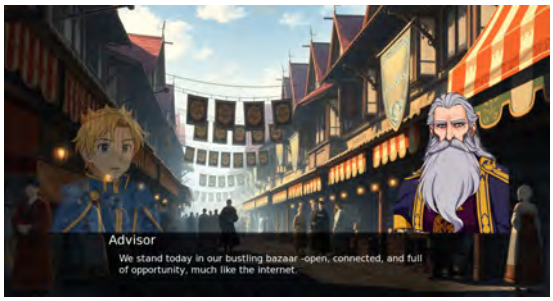

Figure 4.25: Scenario 18

In the last and the final chapter the player interacts with different vendors in a new market (Figure 4.25). This chapter was completely based on telling a story. There were no tasks like before

Figure 4.26: Scenario 19

Figure 4.27: Scenario 20

Figure 4.28: Scenario 21

At first the player interacts with a vendor who offers the player a free rune as a gift. Here the player will have two options. But no matter what is the decision the advisor will intervene and will provide feedback based on the decision of the player. This scenario depicts the **malware** attack. In a malware attack a malicious script hides inside the free crack software or apps and in later on the malicious script continuously harms the device by creating problems [72]. Figure 4.26, Figure 4.27 and Figure 4.28 are some of the scenarios about malware from the game that the players face while playing.

Figure 4.29: Scenario 22

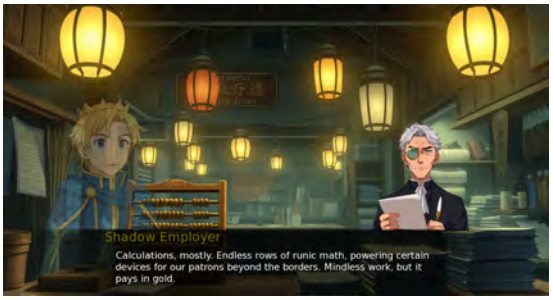

Figure 4.30: Scenario 23

Figure 4.31: Scenario 24

After that the player will interact with a shadow employer. The shadow employer offers work to the people of the city in exchange for gold secretly. Just like the previous one no matter what is the choice the advisor will intervene and will provide feedback to the player. This scenario represents **cryoptojacking**. In cryptojacking, malicious scripts use a device's resource without the permission and the attacker gets all the benefit by mining cryptocurrency [88]. Figure 4.29, Figure 4.30 and Figure 4.31 are some of the scenarios about cryptojacking from the game that the players face while playing.

Figure 4.32: Scenario 25

Figure 4.33: Scenario 26

Figure 4.34: Scenario 27

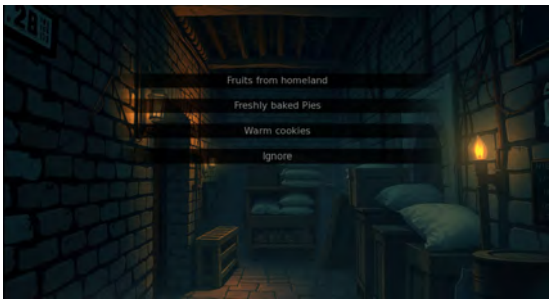

Figure 4.35: Scenario 28

Figure 4.36: Scenario 29

And lastly the player interacts with a cook in a food stall in the bazaar. The cook offers some food items which can be made by tomorrow based on the choice of the prince. But the choice spreads to multiple vendors. Those vendors bombard the player with the same offers again and again. This scenario depicts **malicious pop-up ads**. Just like in the real world when a user's preferences or desires are known harmful sites can offer the same thing based on the users desire. These pop-ups lead to the unwanted interaction as well as unwanted downloads [91]. Figure 4.32 , Figure 4.33 , Figure 4.34, Figure 4.35, Figure 4.36 are some of the scenarios about phishing from the game that the players face while playing.

4.6 In Game Quiz

After each chapter the players faced quizes which were completely based on the game scenarios. For the correct answer the players got 10 points. However for some questions there were the worst possible answers in the option. If the player chooses that option then 5 points would be deducted from the overall point. Some answers were partially correct for those players got 5 points. A player can score upto 100 points. After the choice the players will get immediate feedback no matter what is their choice. The following figures are some quiz questions and feedback. After completing all the three quizes from three chapters the scores get stored in the leaderboard. And the player needs to enter the name when they play the game for the very first time from a browser. However if they want to play the game later on the same browser they do not need to write their name once again. Also as shown in the game flow diagram (Figure 4.7), if the final quiz score is less than 50 then the game is not finished and the player needs to play the game once again. If the final

quiz score is greater than 50 but less than 80 then the player can restart the game to increase the score or can finish the game. Lastly if the score is greater than 80 then the player can finish the game. Figure 4.37, Figure 4.38, Figure 4.39, Figure 4.40, Figure 4.41, Figure 4.42 and Figure 4.43 are some of the quiz questions, feedbacks and leaderboard:

Figure 4.37: Quiz 1

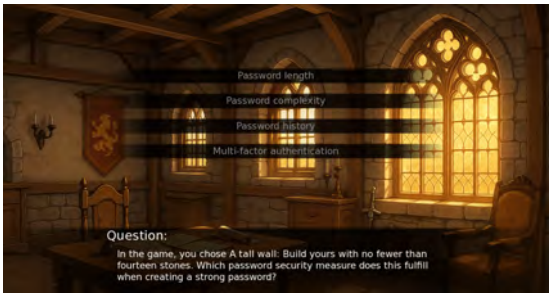

Figure 4.38: Quiz 2

Figure 4.39: Quiz 3

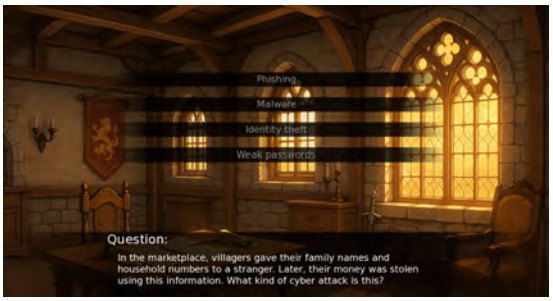

Figure 4.40: Quiz 4

Figure 4.41: Quiz 5

Figure 4.42: Quiz 6

Figure 4.43: Leaderboard

4.7 Game Mechanism and play

Our visual novel game completely implements a choices based system. This system aligns with the decision of players to tackle as well as learning to defend different types of cybersecurity threats. The core mechanics of the game is its dialogue based decision typically presented with choices. Each of the decisions are aligned with specific cybersecurity learning goals. In the game correct choices are rewarded with to progress forward in the game. On the other hand, wrong choices will lead to soft as well as hard failures which reinforce learning through immediate consequences. As mentioned before the gameplay events metaphorically represents different kinds of cybersecurity principles such as building the city defense to reflect the password practices, avoiding or ignoring offers eye catching from a stranger/unknown source by exchanging secret identity reflects identity theft and also differentiation between armor was used to reflect the difference between real website and clone website. Even though they look almost the same, they are actually different. Other scenarios, like interacting with vendors, shadow employers and cook teaches different concepts and a little bit of simulation via story. The game is designed for replayability which encourages players to retry chapters and explore different paths. Successful decisions help players understand cybersecurity better, while failures reveal critical vulnerabilities. With consequence-driven storytelling and metaphorical world-building, the game provides an engaging as well as educational cybersecurity experience.

4.8 Mapping Game Scenario Using Constructivist Learning Theory

The design of our game follows Constructive Learning Theory as mentioned before. Which theory follows that learners will build knowledge through interactive experiences, decision making and reflection. Our game also follows the same principle. Rather than receiving knowledge in boring traditional way, players will gain knowledge with interactive narrative based scenarios. Table 4.1 mentions how our game followed the constructive learning principle till now:

Game Scenario	Cybersecurity Concept	Constructivist Learning Activity
Selecting correct tasks with the builders to rebuild the kingdom's protective wall	Password protection	Hands-on decision making; understanding rules and consequences of strong passwords
Identifying real armor versus fake armor created by the suspicious character	Phishing detection	Pattern recognition; critical observation; evaluating authenticity
Deciding whether to share personal information for "free gold"	Identity theft prevention	Risk assessment; learning from simulated consequences; reflective decision-making
Interacting with vendors offering malicious gifts or software	Malware awareness	Recognizing threats; understanding malware delivery methods; experiential learning
Responding to shadow employer offering hidden crypto-mining tasks	Cryptojacking	Observing covert threats; situational awareness; analyzing resource misuse
Handling repeated pop-up offers in the bazaar	Malicious pop-up ads	Filtering relevant from irrelevant; decision making; experiential learning on user behavior manipulation

Table 4.1: Mapping Game Scenarios to Cybersecurity Concepts using Constructivist Learning Theory

4.9 Depiction of Octalysis Core Drives in the Game

The Octalysis Framework developed by Yu-kai Chou [92] is a comprehensive model for analyzing and designing gamified experiences. It identifies eight core drives of human motivation that influence engagement and behavior. Figure 4.44 is the demonstration of the Octalysis Framework.

Figure 4.44: Octalysis Framework

Table 4.2 illustrates how each core drive which were discussed in the methodology chapter were implemented and depicted in our game:

Octalysis Core Drive	**Depiction in the Game**
Epic Meaning & Calling	The Prince is tasked with rebuilding the kingdom and protecting it from cyber threats. Players feel part of a larger mission, with narrative and high-stakes decisions reinforcing purpose.
Development & Accomplishment	Players track progress through game completion percentages, collect ideas, earn badges, and compare performance via a leaderboard, reinforcing growth and mastery.
Empowerment of Creativity & Feedback	Branching choices, dialogue options, and strategic problem-solving allow experimentation. Players see the outcomes of their decisions, receiving feedback through story consequences.
Ownership & Possession	Quiz scores and based on quiz score the player get feedback about whether they did good or not. Also hidden message after chapter 1. Progression across chapters strengthens personal investment in the game journey.
Social Influence & Relatedness	Leaderboards, advisor and NPC interactions, and recognition in the narrative provide social motivation through comparison, collaboration, and trust-building.
Scarcity & Impatience	Getting hidden message and secret things conversation about threats with advisor create urgency and encourage careful planning.
Unpredictability & Curiosity	What secret lines will replace the scrolls task and unexpected consequences keep players intrigued and motivated to explore.
Loss & Avoidance	Wrong decisions can lead to lost of trust for the villages towards prince or even the collapse of the kingdom. High-stakes consequences motivate careful decision-making.

Table 4.2: Depiction of Octalysis Core Drives in the Game

Chapter 5

Game Evaluation

The evaluation process has been designed as a comparative study between two groups. One is experimental and the other one is the control group. The experimental group interacted with the game which we designed and the control group studied the text based reading material. Both of the group faced screening questions as well as pre-interview questionnaires. After that they interacted with the tutorial or the game and then they faced post interview questionnaires which were similar to pre-interview questionnaires. But post-interview questionnaires were set in order to get detailed answers so that we can evaluate them easily.

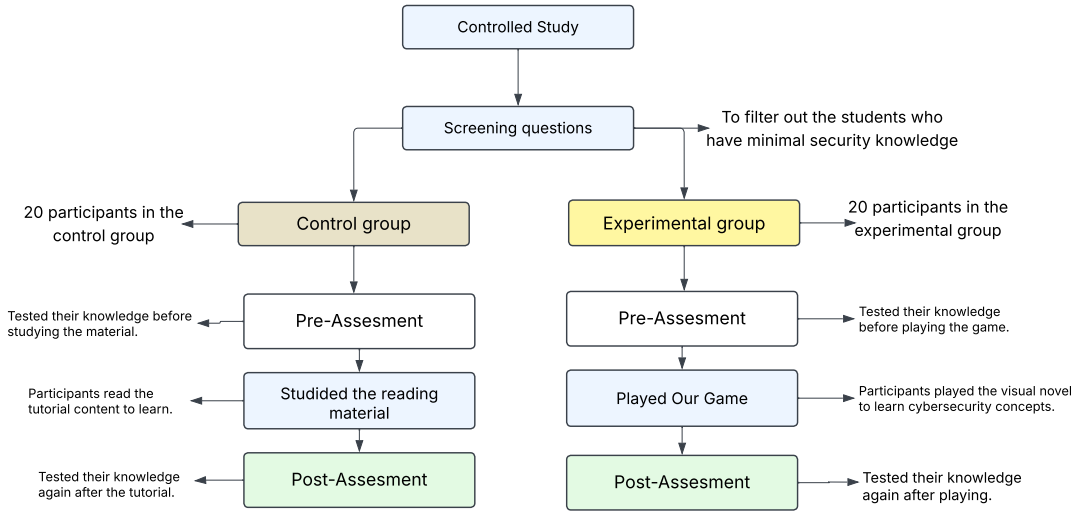

Figure 5.1: Controlled Study Workflow.

5.1 Controlled Study

As mentioned earlier, we conducted a controlled study to evaluate the effectiveness of our game. The goal of this study was to determine how well the game performs in enhancing cybersecurity awareness compared to traditional learning methods. For this purpose, we compared our game-based learning approach with conventional

text-based reading materials, which served as the control condition. The study was designed to observe not only the participants' knowledge improvement but also their level of engagement and motivation throughout the learning process. By introducing both a control group (tutorial-based learning) and an experimental group (game-based learning), we aimed to identify whether gamification can truly make cybersecurity education more interactive, memorable, and impactful. The following sections describe in detail the structure of the study, including participant selection, the materials used, the experimental setup, and the evaluation procedures. This detailed breakdown helps to ensure that the study remains transparent, reproducible, and aligned with the research objectives. Figure 5.1 is the demonstration of the workflow for our controlled study.

5.2 Study Design

The following sections will elaborate on the study design in detail. This structured explanation ensures a clear understanding of how the controlled study was conducted and how the findings were derived.

5.2.1 Screening Questions

We created some screening questions to figure out the technical knowledge of students. As our prior target was the students from the non-technical background with less security knowledge we performed some screening questions as well as pre-interview questionnaires.

We asked them about if they know if they know how to check websites connection secure or not. Also, questions like if have any experience in removing virus and if they participated any kind of seminar regarding cyber security or not.

After getting "No" as answer from all the three questions we selected the participant. We have taken a total number of 40 participants. The participants were selected from the different universities across Bangladesh.

5.2.2 Demographic Questions

The participants were from different departments who have limited interaction with cybersecurity topics. Screening questions ensured that participants had minimal prior knowledge. Also the demographic questions were asked to the participant. We asked about their age, gender, current semester number, department they are currently studying in, years of internet usage and if they play any kind of games or not.

We have maintained an equal ratio based on gender. Also, for the same department, an equal number of participants were in the control group as well as in the experimental group.

5.2.3 Pre-Assessment Procedure

Control and experimental both of the groups faced similar questions on pre-interview. We conducted a structured interview for both the groups and the questions were designed to get binary answers (YES/NO). The interview process was fully voice recorded. The pre-interview was done to evaluate the prior knowledge of the participants. There were a total 20 questions. 3 for password protection, 3 for ransomware, 2 for identity theft, 3 for phishing, 3 for malware, 3 for malicious pop up ads, 3 for cryptojacking. Some of the questions are:

- Do you know about strong password and weak password?
- Do you know about the word malware?
- Do you know about identity theft?

We have also provided unique code for each question to ensure the clarity and easy referencing system throughout the whole analysis. In our code , PP means password protection, R means ransomware, IT means identity theft, P means Phishing, M means malware, CJ means cryptojacking, PUA means malicious pop up ads. This thing made the analysis more easy as well as organized. Table 5.1 is the representation of the code and their meaning

Code	**Meaning**
PP	Password Protection
R	Ransomware
IT	Identity Theft
P	Phishing
M	Malware
CJ	Cryptojacking
PUA	Malicious Popup Ads

Table 5.1: Question Coding Based on Attack

5.2.4 Study Group Activities

As previously mentioned we divided our participants into two different groups. One was the experimental group who will play the game and one was the control group who will read the text based tutorial. After facing the pre-interview questionnaires the printed tutorial was provided to the control group and the game link was provided to the experimental group. Both of the activities were timed as well as monitored by us to ensure consistency.

- Control Group: In the control study, participants were given a detailed text-based cybersecurity tutorial that acted as the non-gamified counterpart to The Exiled Prince. The tutorial was carefully designed to match the game's

content — covering the same cybersecurity topics, learning goals, and real-world scenarios — but delivered through clear, structured written explanations instead of an interactive story. To ensure the material was both accurate and pedagogically sound, the tutorial was developed using well-established cybersecurity awareness frameworks and guidelines (NIST, 2020; FTC, 2024; IBM, 2023; Verizon, 2023). It was divided into seven modules, each focusing on a key area of cybersecurity that also appeared in the game's chapters:

  - **Password Protection:** Explained why strong, unique passwords are vital, the dangers of password reuse, and introduced the use of password managers and multi-factor authentication [45][47][54].
  - **Ransomware**: Described how ransomware attacks work, how they spread, and the best practices for prevention and recovery [68][70][77].
  - **Identity Theft**: Discussed how personal information can be stolen or misused, warning signs of identity fraud, and protective measures like monitoring and MFA [82][75].
  - **Phishing**: Covered how attackers use emails, SMS, and fake websites to deceive users, along with tips for recognizing and avoiding such scams [67][81][77].
  - **Malware**: Explained the different types of malicious software, how infections occur, and practical ways to secure devices [75][46].
  - **Cryptojacking**: Introduced the concept of unauthorized crypto-mining, its symptoms, and steps for detection and prevention [83][46][75].
  - **Malicious Pop-up Ads**: Highlighted how deceptive pop-ups and fake system alerts work, teaching users how to stay cautious online [83][71].

  Each section followed a clear and consistent structure: it defined the threat, explained how it works, identified common warning signs, offered practical prevention and response steps, and cited reliable sources such as NIST [47][46], FTC [82][81][83], IBM [70], Verizon [77] and Symantec [77]. This ensured that all content was factually correct and aligned with recognized global standards. The tutorial was written in simple, easy-to-understand language to make it approachable for non-technical university students. It was presented on multiple pages so participants could scroll through and read at their own pace. Importantly, the tutorial matched the scope and complexity of the game, meaning any difference in learning outcomes between the two groups could be attributed to the mode of delivery not to differences in the quality or depth of the content. In summary, the control condition was not a simplified or weaker version. It was a comprehensive, research-based educational module that conveyed the same cybersecurity lessons as The Exiled Prince, but without the narrative, interactivity, and motivational elements of gamification.

- Experimental Group: The experimental group interacted with the game that we developed. Most of the participants played the game on their own device. They played through all the scenarios as well as faced the inbuilt game quizzes. The game also provided instant feedback based on their choices. The time required for finishing the game for each participant was also recorded. The detail of the game was described in the chapter 4.

5.3 Post interview Procedure

After completing the tutorial or the game both of the group faced the same sets of questionnaires in the post-interview process. While the pre-interview focused on binary answers, the post-interview focused on the detailed answers. This approach helped the evaluator to understand the actual knowledge about the particular cybersecurity topic. Just like the pre-interview questionnaire the post interview questionnaire also had 20 questions. 3 for password protection, 3 for ransomware, 2 for identity theft, 3 for phishing, 3 for malware, 3 for malicious pop up ads, 3 for cryptojacking. Each question has been coded uniquely. Based on the threat the code has been set. In our code , PP means password protection, R means ransomware, IT means identity theft, P means Phishing, M means malware, CJ means cryptojacking, PUA means malicious pop up ads. Table no 5.1 is the demonstration of the code and the meaning of the code. And the number at the end of each code means the number of questions for that particular threat. For an example, P3 means the third question for phishing.This things made the analysis more easy as well as organized. Also we have differently categorized our questions.We have We have mapped our questions into some categories. The category column shows the type of understanding or behavior that each question was designed to measure in this study.

- **Identification** and **Definition** focus on basic knowledge.It focuses on whether participants can understand and clearly describe key cybersecurity terms and concepts.
- **Recognition** and **Evaluation** deal with practical awareness. It demonstrates how well participants can notice signs of threats and make sound judgments about what's safe or unsafe online.
- **Consideration** and **Application** highlight how participants think about cybersecurity in daily life and how they put safe practices into action.
- **Response**, **Prevention** and **Response/Prevention** look at how ready participants are to react properly during a cyber incident or to prevent it from happening in the first place.
- **Consequence** shows whether participants understand the possible risks or damages that can occur from unsafe online actions.
- **Knowledge** represents participants' overall grasp of cybersecurity concepts before and after taking part in the study.

Table 5.2 is the mapping of the category of each question.

Code	Question	Category
PP1	What makes a password strong or weak?	Identification
PP2	What do you consider when creating a password?	Consideration
PP3	What methods for keeping passwords safe?	Application
R1	How would you describe ransomware?	Definition
R2	How would you recognize if a situation was caused by ransomware?	Recognition
R3	What steps would you take if ransomware affected your device?	Response
IT1	What is identity theft? Example?	Definition
IT2	Steps if your identity gets misused?	Response
P1	Explain phishing with example?	Definition
P2	Clues for fake website?	Recognition
P3	Signs before clicking a link (step by step)?	Evaluation
M1	What do you know about malware attacks?	Knowledge
M2	Signs of malware infection?	Recognition
M3	Steps if suspected malware?	Response
PUA1	Risks of "You have a virus" pop-up?	Identification
PUA2	What happens if clicked by mistake?	Consequence
PUA3	Steps to stay safe & why important?	Prevention
CJ1	Explain cryptojacking simply?	Definition
CJ2	Signs of cryptojacking?	Recognition
CJ3	Response & prevention steps?	Response/Prevention

Table 5.2: Interview Questions with Categories

5.4 Data Collection

All of the interviews were voice recorded with the consent of the participant. This was completely done to ensure accuracy while analyzing the data. For all the participants time to complete the game or tutorial and time for the interview was recorded manually with the help of the stopwatch.

5.5 Analysis procedure

The evaluation was done based on the score which has been given based on the answer. For the correct answer the participant got 5 points, for incorrect they got 0 and partially correct they got 2.5 points. After successfully evaluating all the answers all the points were summed up. This summed up point is a score which the participant got in both of the interviews based on their answer. All the evaluations were done by a single evaluator to avoid inconsistency. After that the comparison between control and experimental group was done based on several types of matrices to understand which has actually done well in enhancing the knowledge.

In this part we will analyze all the data which we get from the pre interview and

post interview. We will start analyzing with the demographic analysis.

Demographic Analysis

As mentioned before we have taken an equal number of participants for the control group as well as the experimental group. The control group had 20 participants and the experimental group also had 20 participants. The Figure 5.2 demonstrates the number of the experimental group and the control group.

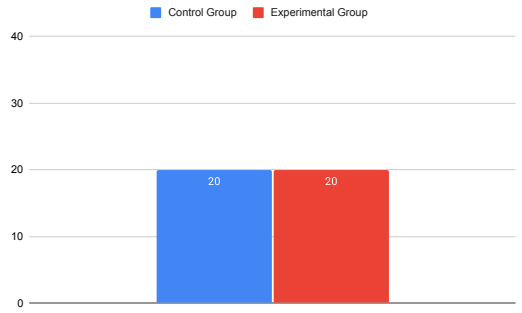

Figure 5.2: Participants in Each Group

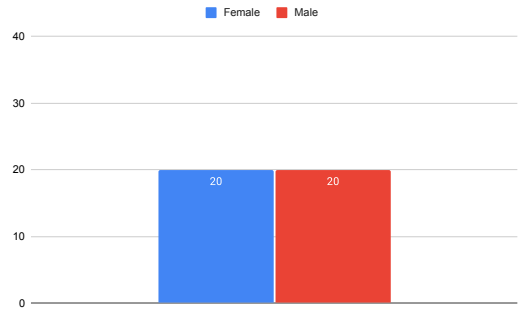

Figure 5.3: Gender Breakdown

Also, as mentioned before we have taken the equal number of male and female ratio. Figure 5.3 demonstrates the number of male and female participants.

We have divided the years of internet use into 3 different groups. Which are 4-6,7-9,10-12,13-16 and 16-18. Where 5 participants are using the internet for 4-6 years, 13 participants are using the internet for 7-9 years, 12 participants are using the internet for 10-12 years, 9 participants are using the internet for 13-15 years and 1 participant has been using the internet for 16-18 years. The figure 5.4 demonstrates the years of internet usage.

And lastly we have also divided age into 4 different groups. Which are 18-20, 21-23, 24-26 and greater than 26. In result we found out 19 students fall in the age group of 21-23 and 21 users fall in the age group of 24-26. Figure 5.5 demonstrates the age group of the participants.

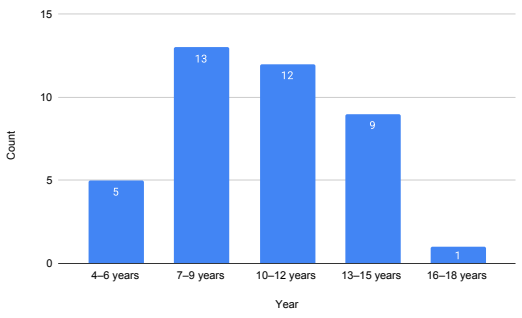

Figure 5.4: Years Of Internet Use

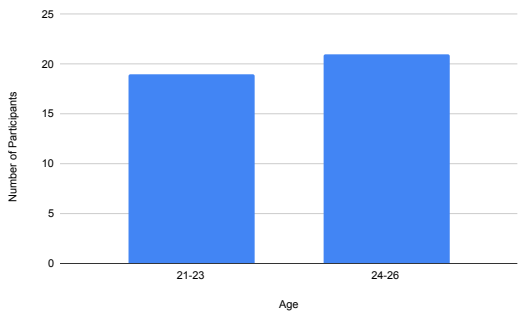

Figure 5.5: Age of the Participants

5.5.1 Analysis of Pre and Post-Interview Questionnaires

Both control group and experiential group faced the same set of questions in the pre interview and post interview. Pre interview questions were made to assess the existing knowledge of the participants. The questions type demanded binary as well as short answers from the user. Table 5.3 is the full analysis of pre interview where based on each question how many correct,partially correct and incorrect answers we got from all the participants is shown.

Question Code	Questions	Correct Count	Partially Correct Count	Incorrect Count
PP1	Do you know about strong or weak passwords?	35	1	4
PP2	When you create a password, how do you usually decide what to use?	31	7	2
PP3	What do you think are the best ways to keep your passwords safe?	12	18	10
R1	Do you know something called ransomware?	8	0	32
R2	Imagine your files or photos got locked, and someone asked for money to give them back. Do you know of any similar cases?	23	1	16
R3	If that happened to you, what would you do?	0	12	28
IT1	Do you know about identity theft?	13	0	27
IT2	What would you do if you found out someone was using your name or account without your permission?	7	29	4
P1	Do you know about phishing attacks?	9	4	27
P2	Have you ever come across a fake website that looked real, where people shared their information and later got into trouble?	27	1	12
P3	If someone sent you a link, how would you figure out if it's real or fake?	5	18	17
M1	Do you know the word malware?	26	2	12

Question Code	Questions	Correct Count	Partially Correct Count	Incorrect Count
M2	Do you know anyone whose phone or laptop suddenly slowed down or started acting strangely after downloading something from a website?	36	2	2
M3	If you thought your device had a virus, what would be the first thing you would do?	15	4	21
PUA1	Some pop-ups look like warnings, for example, 'Your device is infected!' Have you ever seen anything like that? What do you think are the risks or threats associated with such pop-ups?	23	4	13
PUA3	What do you think could happen if you or someone clicks on this kind of pop-up ad?	13	14	13
PUA4	What measures would you take to protect yourself in this kind of situation?	4	24	12
CJ1	Do you know something called cryptojacking?	4	0	36
CJ2	It's when someone secretly uses your computer or phone to mine cryptocurrency. Did you know this was possible?	14	3	23
CJ3	If a website or app was secretly using your device to mine cryptocurrency, what would you do to stop it?	0	5	35

Table 5.3: The Pre-Interview Question Results

After participant finished the game we asked both of the group same sets of questionnaire for post interview. The post interview questionnaire were a little bit tweaked from the pre interview questions. In post interview at first we asked the both group participants

- Would you prefer learning from a game or reading material?

36 of participants said they would prefer learning from a game and only 4 participants said they would prefer reading based tutorials upon the game. However the knowledge of both groups has been enhanced. This was identified based on the score

of their pre interview and post interview. Figure 5.6 demonstrates the enhancement of the participants.

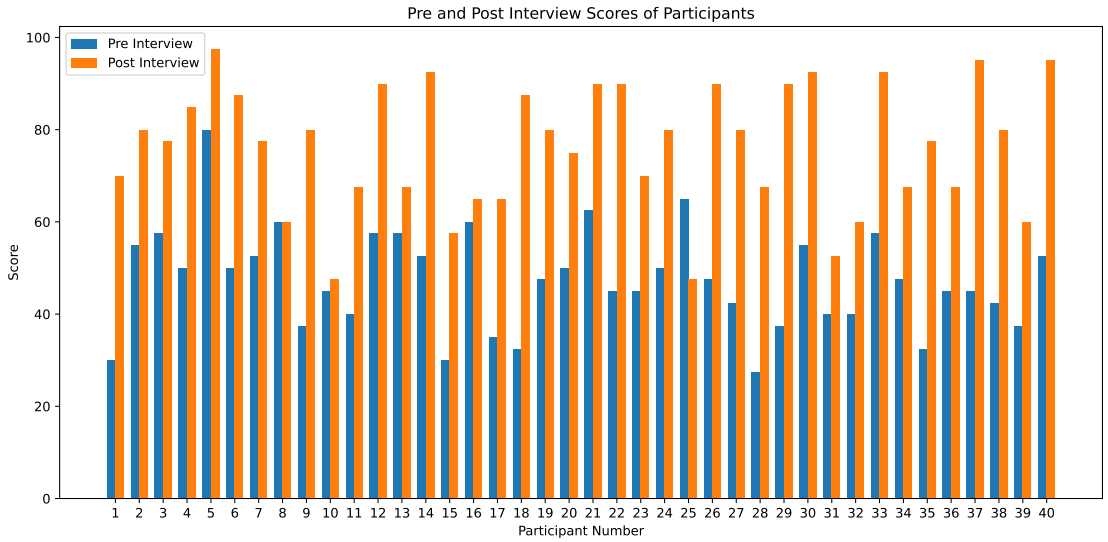

Figure 5.6: Score of the Participants in Pre and Post interview

The questions were focused on to assess the knowledge of the participants. Table 5.4 is the full analysis of post interview where based on each question how many correct,partially correct and incorrect answers we got from the experimental group.

Question Code	**Questions**	**Correct Count**	**Partially Correct Count**	**Incorrect Count**
PP1	How would you explain what makes a password strong or weak? Can you give examples of a strong password?	20	0	0
PP2	What things do you consider when creating a password?	20	0	0
PP3	What methods or strategies for keeping passwords safe do you think are important? How do you apply them?	9	10	1
R1	How would you describe ransomware?	9	5	6
R2	How would you recognize if a situation was caused by ransomware?	7	2	11
R3	What steps would you take if ransomware affected your device?	4	7	9

Question Code	Questions	Correct Count	Partially Correct Count	Incorrect Count
IT1	How would you explain what identity theft means? Can you give an example?	17	0	3
IT2	What steps should be taken if your account or someone else's account you know is being misused?	15	5	0
P1	How would you explain phishing to someone who doesn't know it? Can you give an example of how it works?	10	1	9
P2	What clues would you look for to check if a website is fake?	14	4	2
P3	What signs would you check before clicking a link? Please explain step by step.	7	11	2
M1	What do you know about malware attacks?	11	6	3
M2	What signs would you recognize that suggest a device might be infected with malware?	15	3	2
M3	What exact steps would you take if you suspected your device had malware?	14	2	4
PUA1	Suppose a pop-up appears on your device saying, "You have a virus in your device". What kind of problems or risks could this type of pop-up cause?	10	8	2
PUA2	Suppose you or someone clicked on this pop-up ad by mistake. Do you know what could happen?	10	4	6
PUA3	What steps can a person take to stay safe from this kind of suspicious ads, and why are these steps important?	8	10	2
CJ1	How would you explain cryptojacking in simple words?	4	6	10
CJ2	What signs would you look for to know if your device was being used for cryptojacking?	9	1	10

Question Code	Questions	Correct Count	Partially Correct Count	Incorrect Count
CJ3	Suppose you realized that a website or app was secretly mining cryptocurrency on your device. How would you respond, and what measures would you take to make sure it doesn't happen again?	5	4	11

Table 5.4: The Post-Interview Question Results of Control Group

Also table 5.5 is the full analysis of post interview where based on each question how many correct,partially correct and incorrect answers we got from the control group.

Question Code	Questions	Correct Count	Partially Correct Count	Incorrect Count
PP1	How would you explain what makes a password strong or weak? Can you give examples of a strong password?	20	0	0
PP2	What things do you consider when creating a password?	19	1	0
PP3	What methods or strategies for keeping passwords safe do you think are important? How do you apply them?	18	2	0
R1	How would you describe ransomware?	12	5	3
R2	How would you recognize if a situation was caused by ransomware?	14	3	3
R3	What steps would you take if ransomware affected your device?	10	8	2
IT1	How would you explain what identity theft means? Can you give an example?	20	0	0
IT2	What steps should be taken if your account or someone else's account you know is being misused?	17	2	1

Question Code	Questions	Correct Count	Partially Correct Count	Incorrect Count
P1	How would you explain phishing to someone who doesn't know it? Can you give an example of how it works?	12	5	3
P2	What clues would you look for to check if a website is fake?	20	0	0
P3	What signs would you check before clicking a link? Please explain step by step.	18	1	1
M1	What do you know about malware attacks?	16	2	2
M2	What signs would you recognize that suggest a device might be infected with malware?	16	3	1
M3	What exact steps would you take if you suspected your device had malware?	16	1	3
PUA1	Suppose a pop-up appears on your device saying, "You have a virus in your device". What kind of problems or risks could this type of pop-up cause?	19	1	0
PUA2	Suppose you or someone clicked on this pop-up ad by mistake. Do you know what could happen?	18	2	0
PUA3	What steps can a person take to stay safe from this kind of suspicious ads, and why are these steps important?	18	2	0
CJ1	How would you explain cryptojacking in simple words?	12	4	4
CJ2	What signs would you look for to know if your device was being used for cryptojacking?	17	2	1
CJ3	Suppose you realized that a website or app was secretly mining cryptocurrency on your device. How would you respond, and what measures would you take to make sure it doesn't happen again?	12	5	3

Table 5.5: The Post-Interview Question Results of Experimental Group

5.5.2 Hypothesis Testing

Now to prove after all the analysis we have come up with three hypothesis. We will prove there was actual knowledge enhancement for both groups by **Hypothesis 1** [H1]. Also, we will see which method created more impact by testing **Hypothesis 2** [H2]. Finally, we will go through each security threat to prove whether the game performed better or the tutorial did, which will be tested by **Hypothesis 3** [H3]. The hypothesis are:

1. **Hypothesis 1** :
    - **For Tutorial**:
        - **Null (H_0)** : There is no difference in incorrectness before and after reading the tutorial.
        - **Alternative (H_1)** : There is a difference in the incorrectness before and after the reading the tutorial
    - **For Game**:
        - **Null (H_0)** : There is no difference in incorrectness before and after playing the game.
        - **Alternative (H_1)** : There is a difference in the incorrectness before and after playing the game.
2. **Hypothesis 2**:
    - **Null (H_0)** : After the evaluation there was no difference in the post-interview scores between the control group (tutorial) and the experimental group
    - **Alternative (H_1)** : After the evaluation there was a difference in the post-interview score between the control group (tutorial) and the experimental group (game).
3. **Hypothesis 3** :
    - **Null (H_0)** : The tutorial and game groups had the same distribution of responses (Incorrect, Partial, Correct) for each individual attack.
    - **Alternative (H_1)** : The tutorial and game groups had different distributions of responses (Incorrect, Partial, Correct) for each individual attack.

Hypothesis 1 Testing

To evaluate the effectiveness of the tutorial and gamified interventions in improving cybersecurity awareness, we conducted both within-group and between-group statistical analyses. Each group consisted of 20 participants who completed pre and post intervention interviews assessing their ability to correctly identify and respond to cybersecurity-related attack scenarios. We analyzed the data using paired t-tests to measure within group improvements in pre and post interviews, between group

improvements in post interview and chi-square/Fisher's exact tests to compare distributions of responses (Incorrect, Partial, Correct) between groups across specific cybersecurity threats. For all tests, the significance level threshold was set at $\alpha = 0.05$.

Pre vs Post Interview Analysis (t-tests)

For the **tutorial group**, the null hypothesis (H_0) stated that there would be no difference in the rate of incorrect answers before and after exposure to the tutorial. The alternative hypothesis (H_1) proposed that there would be a difference. A paired t-test yielded a p-value of 3.84×10^{-5}, which is well below the threshold of 0.05. Therefore, we rejected H_0 and based on the conclusion from Figure 5.7 that the tutorial significantly reduced the proportion of incorrect answers. This finding supports the claim that tutorial-based instruction contributes positively to improving cybersecurity awareness.

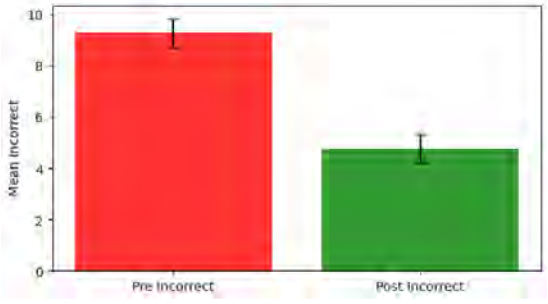

Figure 5.7: Pre vs Post Interview Incorrectness Analysis of Tutorial

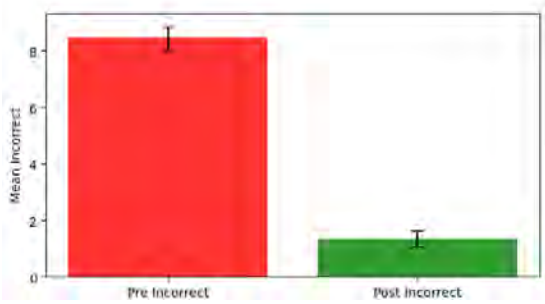

Figure 5.8: Pre vs Post Interview Incorrectness Analysis of Game

For the **game group**, the null hypothesis (H_0) stated that there would be no difference in the rate of incorrect answers before and after playing the game. The alternative hypothesis (H_1) suggested a difference. The paired t-test returned a p-value of 4.79×10^{-12}, again far below 0.05. Thus, H_0 was rejected, and analyzing Figure 5.8 confirms that the game intervention also significantly reduced incorrect responses. Notably, the much smaller p-value relative to the tutorial group ($4.79 \times 10^{-12} << 3.84 \times 10^{-5}$) suggests a stronger effect of the game-based learning approach.

These results confirm that both interventions were effective, but the game-based approach appears to have a stronger influence on reducing errors. This aligns with the expectation that interactive learning environments may engage participants more deeply, leading to more durable knowledge gains.

Hypothesis 2 Testing

For hypothesis 2 [H2] testing we conducted an independent t-test upon the score which we got after the evaluation of participants' interview.

Post-Intervention Comparison: Improvement Between Tutorial and Game (t-test))

To examine the effectiveness of the two training approaches, we compared the score improvements (difference between pre- and post-intervention performance) of participants in the control group (tutorial) and the experimental group (game). The null hypothesis (H_0) stated that there would be no difference in score improvement between the tutorial and game groups following the interventions. Conversely, the alternative hypothesis (H_1) proposed that a significant difference in improvement would exist between the two groups.
The t-test analysis produced a p-value of 3.247×10^{-4}, which is well below the significance threshold of $\alpha = 0.05$. Therefore, we reject the null hypothesis (H_0) and conclude that there is a statistically significant difference in score improvement between participants who engaged with the game and those who followed the tutorial.

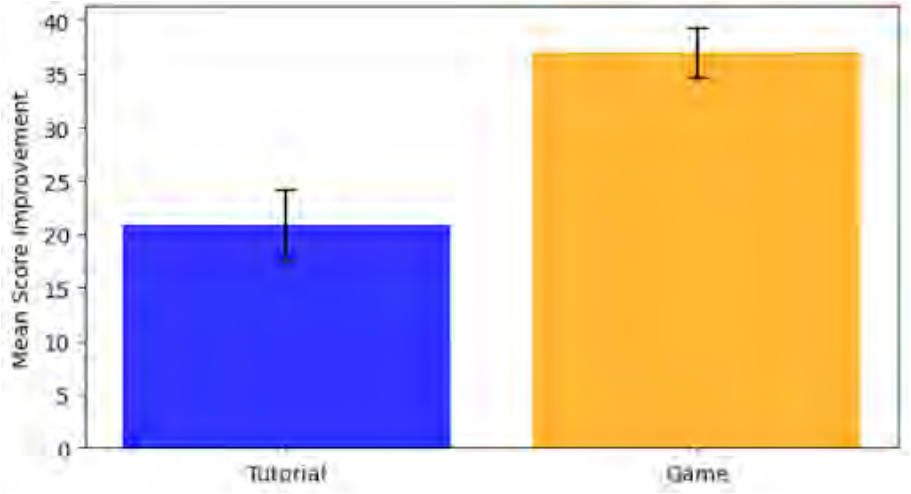

Figure 5.9: Post Intervention Score Improvement Comparison (Tutorial vs. Game)

As shown in Figure 5.9, participants in the game-based learning group demonstrated substantially greater improvement compared to the tutorial group. This finding reinforces the notion that interactive and experiential learning approaches, such as gamified cybersecurity training, can lead to more effective knowledge acquisition and behavioral change than traditional text based tutorials.

Hypothesis 3 Testing

We next compared the distribution of responses (Incorrect, Partial, Correct) between the tutorial and game groups across the seven attack categories (Password Protection, Ransomware, Identity Theft, Malware, Phishing, Pop-up Ads and Cryptojacking).

In order to examine whether the distribution of responses (Incorrect, Partial, Correct) differed between the tutorial group and the game group, we employed both the Chi-square test of independence and Fisher's Exact Test, depending on the characteristics of the data. The Chi-square test is appropriate when the expected frequencies in each cell of the contingency table are sufficiently large (generally $\geqslant 5$) or if any cell frequency=0, as it provides an efficient approximation of the sampling distribution. However, when one or more categories contained very small frequen-

cies, the assumptions of the Chi-square test were not met. In these cases, Fisher's Exact Test was used, as it provides an exact probability calculation and remains valid even with small or uneven cell counts. This dual approach ensured that our statistical conclusions regarding the relationship between training type (tutorial vs. game) and response distributions were both robust and reliable.

The null hypothesis (H_0) for each comparison stated that the distribution of responses would be the same across groups, while the alternative hypothesis (H_1) proposed that the distributions would differ. In order to examine whether the distribution of responses (Incorrect, Partial, Correct) differed between the tutorial group and the game group, we employed both the Chi-square test of independence and Fisher's Exact Test, depending on the characteristics of the data. Table 5.6 gives a clear overview of which cybersecurity threat questions showed differences in response between tutorial and game, and which did not. In the table the questions code is the same code that we mentioned before. As previously Each question has been coded uniquely. Base on the threat the code has been set. In our code , PP means password protection, R means ransomware, IT means identity theft, P means Phishing, M means malware, CJ means cryptojacking, PUA means malicious pop up ads. Table no 5.1 is the demonstration of the code and the meaning of the code. And the number at the end of each code means the number of the question for that particular threat. For example, P3 means the third question for phishing.

Question	**Test Used**	**p-value**	**Decision** ($\alpha = 0.05$)	**Interpretation**
PP1	Fisher Exact	1.0000	Fail to Reject H_0	No difference between groups
PP2	Fisher Exact	1.0000	Fail to Reject H_0	No difference between groups
PP3	Chi-square	0.0094	Reject H_0	Significant difference
R1	Chi-square	0.4895	Fail to Reject H_0	No difference between groups
R2	Chi-square	0.0287	Reject H_0	Significant difference
R3	Chi-square	0.0288	Reject H_0	Significant difference
IT1	Fisher Exact	0.2308	Fail to Reject H_0	No difference between groups
IT2	Fisher Exact	0.6948	Fail to Reject H_0	No difference between groups
P1	Chi-square	0.0537	Fail to Reject H_0	No difference (marginal)
P2	Fisher Exact	0.0202	Reject H_0	Significant difference
P3	Chi-square	0.0012	Reject H_0	Strong significant difference
M1	Chi-square	0.2095	Fail to Reject H_0	No difference between groups
M2	Chi-square	0.5400	Fail to Reject H_0	No difference between groups
M3	Chi-square	0.7373	Fail to Reject H_0	No difference between groups
PUA1	Fisher Exact	0.0033	Reject H_0	Strong significant difference
PUA2	Fisher Exact	0.0138	Reject H_0	Significant difference
PUA3	Fisher Exact	0.0022	Reject H_0	Strong significant difference
CJ1	Chi-square	0.0306	Reject H_0	Significant difference
CJ2	Chi-square	0.0062	Reject H_0	Strong significant difference
CJ3	Chi-square	0.0228	Reject H_0	Significant difference

Table 5.6: Hypothesis 3 Testing Results

When comparing the two approaches, the null hypothesis (H_0) is of "no difference in distributions" was rejected in 5 out of 7 selected scenarios (Password Protection, Ransomware, Phishing, Pop-up Ads and Cryptojacking). These findings suggest that the game-based intervention not only reduced overall incorrectness but also produced different learning patterns in specific threat domains compared to tutorials. The lack of significant differences in Identity Theft and Malware scenarios indicates that both methods were equally effective in those areas. Table 5.7 demonstrates in which attacks our game had advantage and in which attacks both materials performed equally well.

Threat Domain	**Game**	**Tutorial**
Password Protection	✓	
Ransomware	✓	
Identity Theft	✓	✓
Phishing	✓	
Malware	✓	✓
Pop-up Ads	✓	
Cryptojacking	✓	

Table 5.7: Comparison of Game-Based vs Tutorial Approaches Across Threat Domains

Overall, the pattern of results supports the conclusion that while both instructional methods improve cybersecurity awareness, **game** based interventions may yield stronger or more targeted improvements in certain categories of threats, possibly due to their interactive and engaging design.

5.5.3 Discrepancy in User Perception in Understanding

During evaluation we found out in pre-interview multiple participants claimed that they have knowledge about the threat or they know the symptoms of the threat. But after evaluating the post interview we found out the participant actually did not have proper knowledge about the threat. This thing is the Dunning-Kruger effect. The Dunnig-Krugger effect is a cognitive bias where the individuals overestimate their own competence even though they have minimal knowledge about that specific topic [48].

5.5.4 Qualitative Evaluation Data

From the hypothesis testing we can clearly tell the game outperformed the tutorial in terms of effectiveness. However, many users felt the game should be a little bit more different. We got to know this because we asked the users some questions about what they liked and how the game could have been improved. Similarly, we asked the questions to the tutorial readers as well.

One of the participant from the experimental group said:

> *We did enjoy the game because of the interactive learning as well as the visual of the game was very good. Also, the game taught complicated things in a very easy way.*

For what was needed for the game, one participant said:

> *The game could have been a little bit more fun if the music could have been added.*

Also, another participant said:

> *The instructions needed to be a little bit easier and could add more real-life threats to make it better.*

On the other hand, when we asked the participants from the experimental group how the tutorial could be improved, one of them told us that:

> *The tutorials should have more visuals just like the game. If it could have been learned in a more interactive way just like the game, then it would be fun as well as informative.*

This indicates the majority of the users prefer to learn from visual and interactive things like the game. Even though there are many scopes where we could improve our game, visualization and interactivity are key factors which make learning about these attacks easy as well as fun. This has been fulfilled by our game (The Exiled Prince).

5.5.5 Summary

Taken together from figure 5.7, figure 5.8, figure 5.9 and table 5.6, these results show that both tutorial and gamification learning interventions significantly improved cybersecurity awareness within groups, as measured by reductions in incorrect responses. The hypothesis that assumed "no difference between pre and post" were consistently rejected for both interventions, confirming their effectiveness.

Chapter 6

Discussion

Our thesis has been trying to answer all the research questions from the very beginning. Some of the answers were found in the literature review section while some of the answers we found after evaluating and testing our game. This chapter solely focuses on the summarized answers to all the questions and bringing all of them in one place.

RQ1: What is the current level of cybersecurity awareness among university students?

From the literature review we found out the answer to the very first research question of ours. A large number of internet users are university students. But the current level of cybersecurity knowledge among the students is very minimal. Even a large portion of university students still lack basic cybersecurity awareness training, even though they are from computer science (CS) and IT/cybersecurity background.

Also in our study we have designed our pre interview questions to assess the current existing knowledge among the students. And by the result we found out that the existing knowledge is very low among the students. There were a total of 20 questions in our pre interview. The questions were designed in a way to get the binary answer and short answer. After evaluating all the pre interview questions we found out the mean score of the participants. The mean score was 47.4375 which clearly reflects the weak grasp on the basic fundamental cybersecurity topics like password protection, malware,phishing, ransomware, identity theft, cryptojacking and malicious popup ads. These findings indicate the similar things that we found out earlier from the literature review. Findings like this demonstrate that university students actually underestimate learning the basic cybersecurity awareness. Because of the lack of knowledge the students are more vulnerable to these threats as they don't have any idea about the threats as well as they do not know how to protect themselves from these kinds of attacks.

Another thing which we had found out through our research is, most of the participants were using the internet for approximately 10 years. Even though using the internet for such a long period of time the awareness to protect themselves is very minimal. This clearly tells them they are in the online world for a long time but due to the lack of effective resources and content their basic security knowledge has not been improved significantly.

Considering all these things we can finally say that these similar things has also been found out in the literature review which we have done earlier of the thesis. Because our finding from the pre interview certainly aligned with our findings and

also aligns with the findings which we got from the literature review. This thing makes our findings more stronger as other authors found the same things.

RQ2: How do gamified learning methods compare to traditional methods in engaging university students?

In our research we have focused on trying to make an easy and interactive game to create more engagement for the university students. The existing method of teaching such as text based methods and generic educational programs. After the participant finished the game we took user feedback from the participant and based on the participant feedback we found out several things which made our game more engaging than traditional methods.

We asked all the participants after evaluation if they enjoyed our game or not. And 100% of the participants gave us the affirmative answer. Then we asked what things they actually liked about the game. Most of the participants said they loved the interactive learning, as well as the scenario and visuals. Also the players got immediate feedback in the game after each decision. Also the game connects the narrative based story with the real life scenarios. Scenes like creating five strong pillars as well as detecting real armor and fake armor all had different different epic meanings.

These are all things which the participant actually felt good about the game. Because of the interactive learning mechanism, interactive scenario as well as real life example and instant feedback every participant found the game enjoyable. And also because of this reason they will recommend this game to other people who want to learn the same things.

In the literature review from the early stage of the thesis we found out exactly the same things. Our game is actually created based on the early findings of the literature review. In literature review we also found features like leaderboards, scoring, and feedback help motivate students and provide immediate reinforcement, leading to more effective learning and improved behavior. Also teaching the strategies by simulating real-life cybersecurity challenges, allows students to practice skills such as identifying phishing attempts, protecting data, and responding to cyber threats. Furthermore, Gamified tools, such as role-playing, CTF games, and serious games, make cybersecurity education more engaging and enjoyable using interactive scenarios, which helps students better retain information and apply it in real-world scenarios.

So By all these things we can say our finding from the game evaluation clearly aligns with the literature review which. We made our game focusing on the finding of the literature review and eventually we found out that those things actually help to create more engagement towards games for a student.

RQ3: What gamification strategies are effective in improving cybersecurity awareness among university students?

From our study, we found out that creating a scenario based game with the real life example was actually very effective for the student to learn about the basic cyber security attack. As we mentioned before that students are one of the most vulnerable groups regarding cybersecurity awareness, we had to ensure to create an effective as well as fun and eye pleasing game for the students.

From the literature review we found out creating an interactive and engaging learning environment where students can actively participate, face challenges, and receive real-time feedback. This engagement encourages students to learn from both

successes and failures, making the learning process more dynamic and motivating compared to the passive nature of traditional, literature based teaching methods. There are other gamification approaches like- RPG,CTF, Serious games, Simulation based games; all with their own niche benefits and applications. Our findings suggest that gamification offers a more dynamic, effective and enjoyable alternative to traditional methods of education

From our game we found out the same. The beautiful visuals as well as interactive and engaging environment of the game actually helped the students to learn about the security threats. To assess if the participant actually learned or not we asked the similar questions like pre-interview but with some tweak and we got the mean score of 87.25 in the post interview for the experimental group who played the game. This proves the effectiveness. Based on our game we tried to make the scenarios as beautiful as we could, also we made interactive as well as real-time feed backs for the players which made the participants engaged towards our game. Because of the engagement they learned about the security threats which were taught inside the game with real life examples in a very good manner. The effectiveness of the game has been clear when we look into the score of the post interview for the participant who played the game. Also the quiz system also made the game more interesting. In the feedback many users said they felt challenged as well as determination to get a good score which made them learn about the attacks in a better manner.

This finding also indicates that by creating interactive as well as engaging learning environments where students can participate as well as get real time feedback helped the students become more and more enraged towards the game and because of this reason they learned about the threats which we tried to teach towards the game. This thing also aligns with what we found from the literature review.

RQ4: What learning goals are targeted by the implementation of gamification strategies?

Our game focused on teaching the students from non technical backgrounds about basic cybersecurity topics and threats like password protection, identity theft, phishing, malware, ransomware, malicious pop up ads and cryptojacking. Our primary goal was to teach the students about what the attack does, how to detect it and how to prevent it.

From the literature review we found that the primary learning goal targeted by gamification strategies in cybersecurity education is enhancing users' ability to recognize and prevent cyber threats. Another important goal is to develop decision-making and risk management skills. This goal also encompasses training users to understand the consequences of their security choices, fostering a mindset geared towards proactive risk mitigation. Gamification further aims to improve security behaviors and overall cybersecurity awareness among users. In addition to awareness and decision-making, many games target hands-on technical skills and problem-solving abilities.

In our game we also followed the same thing. We targeted to teach the participant about the attack. After that we targeted to teach them how the attack happens and which signs will tell about the attack. Lastly we focused on teaching how the users could keep themselves safe as well as protected from these kinds of attacks. All of the scenarios were mapped to cover all these things. Also several times the player will have the option to simply avoid the threat but in game we created the scenario which also teaches the user what could happen if they just simply avoid it

without letting others know. These all concepts and ideas were found out from the literature review during the early stage of our research.
By following all these things we got a pretty good result which is also mentioned in the previous research question. Our post interview questions were about the definition,identification, prevention or response based on the answer and the score we can say they were successfully able to learn from the game. So in the game we actually focused on creating the ability to recognize the attack, managing the risk and the threats, teaching them the consequences upon their choice and letting other people know about the attack so that they could keep themselves safe from these attacks.

RQ5: What is the audience perception toward gamification?

In our study, we designed our post interview questions in such a way so that we can get to know about the perception about the game. Even though only one group of participants played the game we asked the perception about the game to the both group participants. And the answers were quite similar for all of the participants.
The experimental group participant who played the game we asked them what they would prefer learning from a game or learning from a game. All the participants from the experimental group said they would prefer the game over the tutorial. Then we asked them to justify why they would choose the game. The participants answered that they would prefer interactive learning rather than traditional methods. Because traditional methods are time consuming as well as boring. And most of the participants said they face problems in focusing while learning from a material. On the other hand, as the game is interactive based and scenario based they can learn the same topics from the game rather than wasting their time by reading the traditional methods. Because gamification can be fun as well as helpful to learn a thing, especially complex cybersecurity threats.
After that we asked the same question to the control group participant as well. Out of 20 participants, 16 participants said they would prefer the game over the tutorial which they just finished reading. When we asked what is the reason behind their choice? Most of the answers were quite similar to the participant of the control group. They said learning from a tutorial is boring. But if the same things could be learned from a story based or any kind of game then that would be very fun as well as educational. That's why they prefer games over tutorials.
From the literature review we also found out the same things which we found out from our study. So in summary we can say 36 participants out 40 of our study felt they would learn better and would recommend a game to learn these kinds of security threats. Which clearly indicates a positive perception towards the game.

RQ6: What is the perceived usability of the game among the audience and how does this influence their willingness to complete the security awareness training?

The post-game interviews revealed that the game was perceived very positively by participants. Almost all participants reported that they enjoyed playing the game , and every participant indicated that they would recommend it to others who want to learn about online safety . When asked about the most appreciated features, participants frequently mentioned storytelling and narrative-driven learning , followed by visualization and graphics, interactive engagement, and the ability to deliver information in an accessible way. These findings suggest that the usability of the game was strongly linked to its ability to combine educational content with engaging

delivery methods.
Despite the high overall satisfaction, participants also identified areas for improvement . The most common suggestion was the need for clearer and more structured instructions , followed by the addition of sound or music , more detailed scenarios and content expansion , and simplifying or shortening certain chapters. Importantly, when asked to compare game-based learning to tutorials, the overwhelming majority stated a preference for the game. The reasons cited included better memory retention, higher engagement, and reduced boredom compared to reading-based tutorials. Together, these findings indicate that the game was not only usable and enjoyable but also encouraged greater willingness to engage with cybersecurity training compared to traditional methods. Table 6.1 is the breakdown of our finding for this research question.

Question (Game Group, n=20)	**Main Findings**
Did you enjoy our game?	Majority said Yes (∼95%).
Things liked about the game	Storytelling/Narrative (40%), Visuals/Graphics (30%), Interactive Learning (25%), Informative Content (20%).
Things to improve	Clearer instructions (25%), Add sound/music (15%), More detail/scenarios (15%), Shorter/simplified chapters (10%).
Would you recommend?	All responses said Yes (100%).
Preference (Game vs Tutorial)	Strong preference for Game (∼85%): memory retention, fun, engaging.

Table 6.1: Main findings from the Game Group (n=20)

RQ7: How likely are the audience to apply the knowledge and strategies learned from the game in their personal and academic digital lives?
The interview data also provides evidence that participants are likely to apply the knowledge gained from the game in their personal and academic digital lives. Among tutorial participants, a large majority explicitly expressed a preference for game-based learning, often criticizing tutorials as boring, lengthy, and difficult to remember. Many stated that interactive and practical learning through a game would make it easier to recall and apply cybersecurity knowledge in practice. For instance, one participant noted:

> *"After reading something most of the things we can't remember. So in-game, if we do it practically, it would be better."*

Such statements emphasize the perceived gap between passive reading and active, memorable learning. For the game group, participants frequently highlighted that they retained knowledge more effectively due to the use of scenarios and stories. Several explained that they would be able to apply these lessons to avoid phishing,

scams, or weak password practices in their daily lives. When results from both groups are combined, about 80% of participants indicated that game-based learning was easier to remember and more likely to translate into real-world behavior change. This strongly suggests that the game can not only improve immediate usability and enjoyment but also increase the likelihood of long-term impact in fostering safer digital practices among learners. Table 6.2 demonstrates the preferences of the participants.

Group	**Preference / Reflection**
Tutorial Group (n=20)	∼75% would prefer Game over tutorial, citing interactivity, better memory, and practical learning.
Game Group (n=20)	Majority (∼80–90%) noted improved recall via stories and scenarios; believed lessons would apply to real life.
Combined (n=40)	∼80% agreed that game-based learning is easier to remember and more likely to influence real behavior (phishing, scams, password safety, etc.).

Table 6.2: Participants' preferences and reflections on game-based vs. tutorial learning.

Chapter 7

Conclusion

To conclude, Cybersecurity threats have become a major concerning issue in recent years. It is evolving day by day. And students are very much vulnerable to these kinds of cyber threats as a large number of internet users are the students. But traditional methods could not grab the attention of this younger group of people that's why they remained vulnerable to the security threats.

Our research successfully demonstrated that a gamified solution is better even though the demography is different. In our research we developed a visual novel game called "The Exiled Prince" which integrates the real world cyber threats in an interacting scenario based fun game. We tried to develop the game by fulfilling the necessary criteria of constructive learning mechanism and the octalysis framework. So that, we could make a better user friendly game.

In our research we found out that the existing traditional education methods fail to capture the attention of the young learners for the most of the time. Because of this reason this group of people remain vulnerable to different kind of cyber threats.

Our research tried to fulfill that gap. We have conducted a study on two groups which are 1.Control group and 2. Experimental group. The control group studied the reading material and the experimental group got to interact with the game. There were a total of 40 students of non-technical background who participated in our study and each group had the equal number of participants to ensure fair assessment. To play our game there is no need for heavy resources. It is just a simple visual novel game. While this study focused on non-CS university students, The Exiled Prince can also be used as a teachable for any non-technical individual wanting to increase their cybersecurity awareness.

Our user study showed a tremendous improvement than the traditional reading methods. The user study was also conducted by two different interviews to assess the knowledge properly. This work contributes to HCI and educational tools by providing a scalable as well as easy. Our game not only educates the student but also it promotes the gamified learning approach in Bangladesh. As digital threats are evolving day by day this kind of method has become very much necessary.

7.1 Limitations

Even though our study showed a promising result the number of participants were relatively low. We take evaluation from a total of 40 students. Because of time limitations we could not extend the number of participants in our evaluation process. Also we failed to add any kind of animations as well as music in our game. Also the study was conducted over a short period of time. Long term retention of knowledge was not measured. Because of this reason we can not tell if the method is effective in the long run or not.
Also because of the time limitation we could only compare our game with the text based methods. There are other methods which also need to be compared in the long run.
Also because of the limited resources the game visualization could not be improved. As all the characters and background images were generated via image generator using prompt for free we actually could not generate more than 2 or 3 three reactions per character. If we could hire an artist then the visualization could have been better.

7.2 Future work

As many participants demanded music could make the game better we will add music as well as animations in the future. Also we will try to assess our game in long term retention. We will try to make the game in multiple languages so that users who do not have proficiency in English can also play.
In the future, the game can be extended and tested for a larger group beyond university students. While the current study primarily targeted non-CS university students, the nature of The Exiled Prince's design enables it to be played by any non-professional or non-CS student. Future research can target making the content finer, language easier, and difficulty levels easier for individuals of varying ages, professions, and educations so that the game can reach and be popular beyond academic communities and support across the country towards cybersecurity awareness.
Furthermore, we will conduct the assessment on a large scale in the future. We will continuously try to update the game with new attacks or we will update the same attack with different scenarios.
To conclude, we will try to make the UI as smooth as possible and will also try to add different kinds of feedback other than the text based feedback. Also we will try to integrate the game into different kinds of workshops for university students.

References

[1] J. Bruner, *Toward a Theory of Instruction* (Belknap Press). Harvard University Press, 1966, ISBN: 9780674897014. [Online]. Available: https://books.google.com.bd/books?id=F_d96D9FmbUC.

[2] J. Piaget, "To understand is to invent: The future of education," 1973.

[3] C. E. Irvine, M. F. Thompson, and K. Allen, "Cyberciege: Gaming for information assurance," *IEEE Security & Privacy*, vol. 3, no. 3, pp. 61–64, 2005.

[4] S. Sheng et al., "Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish," in *Proceedings of the 3rd symposium on Usable privacy and security*, 2007, pp. 88–99.

[5] J. Idziorek, M. F. Tannian, and D. W. Jacobson, "Teaching computer security literacy to students from non-computing disciplines," in *2011 ASEE Annual Conference & Exposition*, 2011, pp. 22–1379.

[6] A. Nagarajan, J. M. Allbeck, A. Sood, and T. L. Janssen, "Exploring game design for cybersecurity training," in *2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, IEEE, 2012, pp. 256–262.

[7] G. Bauer, D. Martinek, S. Kriglstein, G. Wallner, and R. Wölfle, "Digital game-based learning with "internet hero"," *Context Matters!*, p. 148, 2013.

[8] T. Denning, A. Lerner, A. Shostack, and T. Kohno, "Control-alt-hack: The design and evaluation of a card game for computer security awareness and education," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 2013, pp. 915–928.

[9] W. Ryan, J. Stewart, D. Verleger, and J. Crofts, "Network nightmares: Using games to teach networks and security.," in *FDG*, 2013, pp. 413–416.

[10] J. Hamari, J. Koivisto, and H. Sarsa, "Does gamification work? – a literature review of empirical studies on gamification," in *2014 47th Hawaii International Conference on System Sciences*, 2014, pp. 3025–3034. DOI: 10.1109/HICSS.2014.377.

[11] J. Mirkovic and P. A. Peterson, "Class {capture-the-flag} exercises," in *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, 2014.

[12] M. Olano et al., "{Securityempire}: Development and evaluation of a digital game to promote cybersecurity education," in *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, 2014.

[13] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki, "A review of using gaming technology for cyber-security awareness," *Int. J. Inf. Secur. Res.(IJISR)*, vol. 6, no. 2, pp. 660–666, 2016.

[14] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki, "A survey of cyber-security awareness in saudi arabia," in *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, IEEE, 2016, pp. 154–158.

[15] M. Hendrix, A. Al-Sherbaz, and B. Victoria, "Game based cyber security training: Are serious games suitable for cyber security training?" *International Journal of Serious Games*, vol. 3, no. 1, pp. 53–61, 2016.

[16] T. Hunt, "Cyber security awareness in higher education," 2016.

[17] D. Sarathchandra, K. Haltinner, and N. Lichtenberg, "College students' cybersecurity risk perceptions, awareness, and practices," in *2016 Cybersecurity Symposium (CYBERSEC)*, 2016, pp. 68–73. DOI: 10.1109/CYBERSEC.2016.018.

[18] N. Ahmed, U. Kulsum, M. Azad, Z. Momtaz, and E. Haque, "Cybersecurity awareness survey: An analysis from bangladesh perspective," Dec. 2017, pp. 788–791. DOI: 10.1109/R10-HTC.2017.8289074.

[19] E. Gjertsen, E. A. Gjære, M. Bartnes, and W. Rocha Flores, "Gamification of information security awareness and training," Jan. 2017, pp. 59–70. DOI: 10.5220/0006128500590070.

[20] K. Leune and S. J. Petrilli Jr, "Using capture-the-flag to enhance the effectiveness of cybersecurity education," in *Proceedings of the 18th annual conference on information technology education*, 2017, pp. 47–52.

[21] K. Senthilkumar and S. Easwaramoorthy, "A survey on cyber security awareness among college students in tamil nadu," in *Iop conference series: Materials science and engineering*, IOP Publishing, vol. 263, 2017, p. 042 043.

[22] D. Aladawy, K. Beckers, and S. Pape, "Persuaded: Fighting social engineering attacks with a serious game," in *Trust, Privacy and Security in Digital Business: 15th International Conference, TrustBus 2018, Regensburg, Germany, September 5–6, 2018, Proceedings 15*, Springer, 2018, pp. 103–118.

[23] G. CJ, S. Pandit, S. Vaddepalli, H. Tupsamudre, V. Banahatti, and S. Lodha, "Phishy-a serious game to train enterprise users on phishing awareness," in *Proceedings of the 2018 annual symposium on computer-human interaction in play companion extended abstracts*, 2018, pp. 169–181.

[24] H. Enriquez, Y. Kadobayashi, and D. Fall, "Project config. play a turn-based strategy security board game," in *Proceedings of the 12th European conference on games based learning (ECGBL 2018)*, 2018, pp. 72–81.

[25] W. Kijpoonphol and W. Phumchanin, "A comparison between traditional and gamified teaching methods for phrasal verb: A case of grade 10 students," *TESOL International Journal*, vol. 13, pp. 56–65, Jan. 2018.

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

[27] A. Moallem, "Cyber security awareness among college students," in *International conference on applied human factors and ergonomics*, Springer, 2018, pp. 79–87.

[28] I. A. Tøndel, T. D. Oyetoyan, M. G. Jaatun, and D. Cruzes, "Understanding challenges to adoption of the microsoft elevation of privilege game," in *Proceedings of the 5th Annual Symposium and Bootcamp on Hot Topics in the Science of Security*, 2018, pp. 1–10.

[29] E. Zoto, S. J. Kowalski, B. Katt, C. Frantz, and E. A. Lopez Rojas, "Cyberaims: A tool for teaching adversarial and systems thinking," in *International Defence and Homeland Security Simulation Workshop, DHSS 2018*, DIME UNIVERSITÀ DI GENOVA, DIMEG UNIVERSITY OF CALABRIA Genoa, 2018.

[30] M. Bada, A. M. Sasse, and J. R. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?" *arXiv preprint arXiv:1901.02672*, 2019.

[31] C. Mio, E. Ventura-Medina, and E. Joao, "Scenario-based elearning to promote active learning in large cohorts: Students' perspective," *Computer Applications in Engineering Education*, vol. 27, no. 4, pp. 894–909, 2019.

[32] C. Mio, E. Ventura-Medina, and E. João, "Scenario-based elearning to promote active learning in large cohorts: Students' perspective," *Computer Applications in Engineering Education*, vol. 27, Jun. 2019. DOI: 10.1002/cae.22123.

[33] T. Omiya, D. Fall, and Y. Kadobayashi, "Iot-poly: An iot security game practice tool for learners motivation and skills acquisition," in *Proceedings of the 19th Koli Calling International Conference on Computing Education Research*, 2019, pp. 1–10.

[34] T. Omiya and Y. Kadobayashi, "Secu-one: A proposal of cyber security exercise tool for improving security management skill," in *Proceedings of the 2019 7th International Conference on Information and Education Technology*, ser. ICIET 2019, Aizu-Wakamatsu, Japan: Association for Computing Machinery, 2019, pp. 259–268, ISBN: 9781450366397. DOI: 10.1145/3323771.3323792. [Online]. Available: https://doi.org/10.1145/3323771.3323792.

[35] S. Scholefield and L. A. Shepherd, "Gamification techniques for raising cyber security awareness," in *HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings 21*, Springer, 2019, pp. 191–203.

[36] Z. A. Wen, Z. Lin, R. Chen, and E. Andersen, "What. hack: Engaging anti-phishing training through a role-playing phishing simulation game," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–12.

[37] D. Aljeaid, A. Alzhrani, M. Alrougi, and O. Almalki, "Assessment of end-user susceptibility to cybersecurity threats in saudi arabia by simulating phishing attacks," *Information*, vol. 11, no. 12, 2020, ISSN: 2078-2489. DOI: 10.3390/info11120547. [Online]. Available: https://www.mdpi.com/2078-2489/11/12/547.

[38] H. Alqahtani and M. Kavakli-Thorne, "Design and evaluation of an augmented reality game for cybersecurity awareness (cybar)," *Information*, vol. 11, no. 2, p. 121, 2020.

[39] M. Anft, "An emerging threat: Ransomware," *The Chronicle of Higher Education*, 2020.

[40] J. Chen, J. Ma, and R. Huang, "Intelligent visual similarity-based phishing websites detection," *Symmetry*, vol. 12, no. 10, p. 1681, 2020. [Online]. Available: https://www.mdpi.com/2073-8994/12/10/1681.

[41] T. Chen, M. Stewart, Z. Bai, E. Chen, L. Dabbish, and J. Hammer, "Hacked time: Design and evaluation of a self-efficacy based cybersecurity game," in *Proceedings of the 2020 acm designing interactive systems conference*, 2020, pp. 1737–1749.

[42] 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, Apr. 2020. DOI: 10.1016/j.cose.2020.101827.

[43] Kaspersky Lab, *Kaspersky disconnected*, Digital game, Educational cybersecurity game available from Kaspersky Lab, 2020. [Online]. Available: https://www.kaspersky.com/disconnected.

[44] J. Koivisto and A. Malik, "Gamification for older adults: A systematic literature review," *The Gerontologist*, vol. 61, no. 7, e360–e372, Jun. 2020, ISSN: 0016-9013. DOI: 10.1093/geront/gnaa047. eprint: https://academic.oup.com/gerontologist/article-pdf/61/7/e360/40357921/gnaa047.pdf. [Online]. Available: https://doi.org/10.1093/geront/gnaa047.

[45] Microsoft Security, "Multi-factor authentication: A necessity in modern security," Microsoft, Tech. Rep., 2020. [Online]. Available: https://www.microsoft.com/security/blog.

[46] National Institute of Standards and Technology (NIST), "Cybersecurity framework," U.S. Department of Commerce, Tech. Rep., 2020. [Online]. Available: https://www.nist.gov/cyberframework.

[47] National Institute of Standards and Technology (NIST), "Digital identity guidelines: Authentication and lifecycle management (sp 800-63b)," U.S. Department of Commerce, Tech. Rep., 2020. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63b.html.

[48] D. Pilat. "Dunning–kruger effect." Accessed: 2025-10-03, The Decision Lab. [Online]. Available: https://thedecisionlab.com/biases/dunning-kruger-effect.

[49] P. Prinetto, G. Roascio, and A. Varriale, "Hardware-based capture-the-flag challenges," in *2020 IEEE East-West Design & Test Symposium (EWDTS)*, IEEE, 2020, pp. 1–8.

[50] S. Ros, S. González, A. Robles, L. Tobarra, A. Caminero, and J. Cano, "Analyzing students' self-perception of success and learning effectiveness using gamification in an online cybersecurity course," *IEEE Access*, vol. 8, pp. 97 718–97 728, 2020. DOI: 10.1109/ACCESS.2020.2996361.

[51] K. H. Sharif and S. Y. Ameen, "A review of security awareness approaches with special emphasis on gamification," in *2020 International conference on advanced science and engineering (ICOASE)*, IEEE, 2020, pp. 151–156.

[52] S. V. Veneruso, L. S. Ferro, A. Marrella, M. Mecella, and T. Catarci, "Cybervr: An interactive learning experience in virtual reality for cybersecurity related issues," in *Proceedings of the 2020 International Conference on Advanced Visual Interfaces*, 2020, pp. 1–8.

[53] T. F. Ask, B. J. Knox, R. Lugo, L. Hoffmann, and S. Sütterlin, "A gamification approach to improving interpersonal situational awareness in cyber defense," 2021.

[54] P. G. Kelley et al., "Password management strategies for online accounts," *ACM Transactions on Information and System Security*, vol. 24, no. 4, pp. 1–35, 2021. DOI: 10.1145/3428475.

[55] M. Khader, M. Karam, and H. Fares, "Cybersecurity awareness framework for academia," *Information*, vol. 12, p. 417, Oct. 2021. DOI: 10.3390/info12100417.

[56] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, 2021.

[57] National Institute of Standards and Technology (NIST), *Human centered design (hcd)*, NIST, U.S. Department of Commerce, Created April 12, 2021; Updated May 3, 2021, 2021. [Online]. Available: https://www.nist.gov/itl/iad/visualization-and-usability-group/human-factors-human-centered-design.

[58] T. Steen and J. Deeleman, "Successful gamification of cybersecurity training," *Cyberpsychology, Behavior, and Social Networking*, vol. 24, Sep. 2021. DOI: 10.1089/cyber.2020.0526.

[59] R. Dillon and Arushi, ""perihack": Designing a serious game for cybersecurity awareness," in *2022 IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE)*, 2022, pp. 630–634. DOI: 10.1109/TALE54877.2022.00108.

[60] F. B. Fatokun, Z. A. Long, S. Hamid, J. O. Fatokun, C. I. Eke, and A. Norman, "Gamifying cybersecurity knowledge to promote good cybersecurity behaviour," *Journal of Computing Technologies and Creative Content (JTec)*, vol. 7, no. 2, pp. 25–34, 2022.

[61] A. FILIPPIDIS, T. Lagkas, H. Mouratidis, S. Nifakos, E. Grigoriou, and P. Sarigiannidis, "Enhancing information security awareness programs through collaborative learning," in *European Conference on Games Based Learning*, vol. 16, 2022, pp. 803–810.

[62] P. Kulkarni, P. Gokhale, Y. Satish, and B. Tigadi, "An empirical study on the impact of learning theory on gamification-based training programs," *Organization Management Journal*, vol. 19, Mar. 2022. DOI: 10.1108/OMJ-04-2021-1232.

[63] J. Morais, J. Simões, J. Lorenço, and S. F. S. F. Lopes, "Perceptions on gamification towards cybersecurity literacy: Social sustainability of educative projects," *Revista EDaPECI*, vol. 22, no. 3, pp. 63–77, 2022.

[64] J. Nijland, "Gamification of cyber security awareness training for phishing against university students," B.S. thesis, University of Twente, 2022.

[65] L. Thompson, N. Melendez, J. Hempson-Jones, and F. Salvi, "Gamification in cybersecurity education: The rad-sim framework for effective learning," *European Conference on Games Based Learning*, vol. 16, pp. 562–569, Oct. 2022. DOI: 10.34190/ecgbl.16.1.504.

[66] T. Williams and O. El-Gayar, "Design of a virtual cybersecurity escape room," in *National Cyber Summit (NCS) Research Track 2021*, Springer, 2022, pp. 60–73.

[67] Anti-Phishing Working Group (APWG), "Phishing activity trends report," APWG, Tech. Rep., 2023. [Online]. Available: https://apwg.org.

[68] Federal Bureau of Investigation (FBI), "Ransomware prevention and response for cisos," FBI, Tech. Rep., 2023. [Online]. Available: https://www.fbi.gov.

[69] K. Hilliard Jr, "Using gamification to enhance mastery of network security concepts," M.S. thesis, North Carolina Agricultural and Technical State University, 2023.

[70] IBM Security, "Cost of a data breach report 2023," IBM, Tech. Rep., 2023. [Online]. Available: https://www.ibm.com/reports/data-breach.

[71] Kaspersky, "Malvertising and pop-up scams explained," Kaspersky Lab, Tech. Rep., 2023. [Online]. Available: https://www.kaspersky.com.

[72] Kaspersky. "Trojan malware hidden in cracked macos software, kaspersky says." Accessed: 2025-10-02. [Online]. Available: https://securityboulevard.com/2023/12/trojan-malware-hidden-in-cracked-macos-software-kaspersky-says/.

[73] N. Kshetri, D. Hoxha, et al., "Knowcc: Knowledge, awareness of computer & cyber ethics between cs/non-cs university students," in *2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, IEEE, 2023, pp. 298–304.

[74] O. Mason, S. Collman, S. Kazamia, and I. Boureanu, "Preparing uk students for the workplace: The acceptability of a gamified cybersecurity training," *Journal of Cybersecurity Education Research and Practice*, vol. 2024, Oct. 2023. DOI: 10.32727/8.2023.35.

[75] Symantec, "Internet security threat report," Symantec Corporation, Tech. Rep., 2023.

[76] The Business Standard, *Internet users in bangladesh reach 131 million in 2023*, Accessed: 1 Feb. 2025, 2023. [Online]. Available: https://www.tbsnews.net/bangladesh/internet-users-bangladesh-reach-131-million-2023-791442.

[77] Verizon Enterprise, "2023 data breach investigations report," Verizon, Tech. Rep., 2023. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/.

[78] H. Xiao, H. Wei, Q. Liao, Q. Ye, C. Cao, and Y. Zhong, "Exploring the gamification of cybersecurity education in higher education institutions: An analytical study," in *SHS Web of Conferences*, EDP Sciences, vol. 166, 2023, p. 01 036.

[79] F. Abraham, *Cyber Smart: YOUR GUIDE TO ONLINE SECURITY AND RESPONSIBILITY*. Jun. 2024.

[80] Check Point Software Technologies, *Cyber security report 2024*, Accessed: 2025-10-03, 2024. [Online]. Available: https://www.checkpoint.com/security-report/?flz-category=items&flz-item=report--cyber-security-report-2024&_gl=1*3j7eei*_gcl_au*NTQ3MzM4NTIzLjE3NTk0NDI1ODA.

[81] Federal Trade Commission (FTC), "How to recognize and avoid phishing scams," FTC, Tech. Rep., 2024. [Online]. Available: https://consumer.ftc.gov.

[82] Federal Trade Commission (FTC), "Identity theft: What to know, what to do," FTC, Tech. Rep., 2024. [Online]. Available: https://consumer.ftc.gov.

[83] Federal Trade Commission (FTC), "Pop-up ads and scams: How to protect yourself," FTC, Tech. Rep., 2024. [Online]. Available: https://consumer.ftc.gov.

[84] K. Hilliard, X. Yuan, K. Bryant, J. Xu, and Z. Jinghua, "Using gamification to enhance mastery of network security concepts," *Journal of Cybersecurity Education, Research and Practice*, vol. 2024, Jul. 2024. DOI: 10.62915/2472-2707.1187.

[85] G. Tempestini, S. Mer
, 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.

[86] Tom Rothamel, *Ren'py visual novel engine*, https://www.renpy.org/, Version 8.2.0, Accessed: 2025-10-01, 2024.

[87] L. Williams, E. Anthi, Y. Cherdantseva, and A. Javed, "Leveraging gamification and game-based learning in cybersecurity education: Engaging and inspiring non-cyber students," in *Journal of The Colloquium for Information Systems Security Education*, vol. 11, 2024, pp. 8–8.

[88] Kaspersky. "What is cryptojacking and how does it work?" Accessed: 2025-10-02. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cryptojacking.

[89] H. Osborne, "'free hamper – just pay p&p': The scam offers targeting your bank details," *The Guardian*, May 2025, Accessed: 2025-10-02. [Online]. Available: https://www.theguardian.com/money/2025/may/18/youve-been-chosen-what-to-do-replied-fake-email-advert-scammer.

[90] V. Rikkers and D. K. Sarmah, "A story-driven gamified education on usb-based attack," *Journal of Computing in Higher Education*, vol. 37, no. 1, pp. 248–272, 2025.

[91] Trend Micro. "How to identify and remove fake pop-ups." Accessed: 2025-10-02. [Online]. Available: https://helpcenter.trendmicro.com/en-us/article/tmka-05037.

[92] Y.-k. Chou, *The octalysis framework for gamification & behavioral design*, https://yukaichou.com/gamification-examples/octalysis-complete-gamification-framework/, Accessed: 2025-10-02.

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

[94] *Netlify: Cloud platform for modern web projects*, https://www.netlify.com/, Accessed: 2025-10-01.

Appendix

Informed Consent Form For the Control Group

Identification of Researchers: This research is being supervised by Dr. Farida Chowdhury. We are affiliated with BRAC University.
Purpose of the Study: The purpose of this study is to develop and evaluate a visual novel game designed to enhance cybersecurity awareness and knowledge among university students in Bangladesh which encourage better understanding and adoption of safe online practices.
Request for Participation: We invite you to take part in an evaluation related to our study on gamified cybersecurity awareness for university students in Bangladesh. Your participation is completely voluntary, and choosing not to participate will not result in any penalties or negative consequences. You are free to stop participating at any time or skip any questions you prefer not to answer. You may also request to withdraw your data at the end of the study by informing the research team.
Exclusions: You must be at least 18 years of age to participate in this study.
Description of Research Method: This study involves participating in a short evaluation process, which will take approximately one to two hours to complete. First, you will be asked a few questions to assess your current security knowledge. Then, you will read a tutorial on security concepts, prepared from existing text-based learning materials. A printed copy of the tutorial will be provided to you. After completely reading the tutorial, you will be asked some questions again to measure if there is any change in your knowledge. At the end of the session, you will have an opportunity to ask any questions. With your permission, we will audio record the conversation for research purposes.
Privacy: All the stored information will be anonymous. We will not record your name or any information that could be used to identify you from any other participant. At the end of the evaluation, your data will be stored and indistinguishable from any other participants.
Explanation of Risks: There are no risks to you personally to give this evaluation.
Explanation of Benefits: You will be able to know more about the impact of technology on the society/your profession/your community after taking part in this study.
Compensation: If this is a financially compensated study, you will receive 300 Tk, based on the nature of your participation.
Questions: If you have any questions about this study, please contact Dr. Farida Chowdhury at farida.chowdhury@bracu.ac.bd.
If you would like to participate, please sign a copy of this letter and return it to me. The other copy is for you to keep.

I have read this letter and agree to participate.
Signature: _____
Printed Name: _____
Date: _____

Person Obtaining Consent: _____

Informed Consent Form For the Experimental Group

Identification of Researchers: This research is being supervised by Dr. Farida Chowdhury. We are affiliated with BRAC University.
Purpose of the Study: The purpose of this study is to develop and evaluate a visual novel game designed to enhance cybersecurity awareness and knowledge among university students in Bangladesh which encourage better understanding and adoption of safe online practices.
Request for Participation: We invite you to take part in an evaluation related to our study on gamified cybersecurity awareness for university students in Bangladesh. Your participation is completely voluntary, and choosing not to participate will not result in any penalties or negative consequences. You are free to stop participating at any time or skip any questions you prefer not to answer. You may also request to withdraw your data at the end of the study by informing the research team.
Exclusions: You must be at least 18 years of age to participate in this study.
Description of Research Method: This study involves participating in a short evaluation process, which will take approximately one to two hours to complete. First, you will be asked a few questions to assess your current security knowledge. Then, you will read a tutorial on security concepts, prepared from existing text-based learning materials. A printed copy of the tutorial will be provided to you. After completely reading the tutorial, you will be asked some questions again to measure if there is any change in your knowledge. At the end of the session, you will have an opportunity to ask any questions. With your permission, we will audio record the conversation for research purposes.
Privacy: All the stored information will be anonymous. We will not record your name or any information that could be used to identify you from any other participant. At the end of the evaluation, your data will be stored and indistinguishable from any other participants.
Explanation of Risks: There are no risks to you personally to give this evaluation.
Explanation of Benefits: You will be able to know more about the impact of technology on the society/your profession/your community after taking part in this study.
Compensation: If this is a financially compensated study, you will receive 300 Tk, based on the nature of your participation.
Questions: If you have any questions about this study, please contact Dr. Farida Chowdhury at farida.chowdhury@bracu.ac.bd.
If you would like to participate, please sign a copy of this letter and return it to me. The other copy is for you to keep.

I have read this letter and agree to participate.
Signature: _____
Printed Name: _____
Date: _____

Person Obtaining Consent: _____

Screening Questions

1. Do you know how to check if a website's connection is secure?
2. Have you ever helped someone remove a virus from their computer or device?
3. Have you ever attended a seminar or session on cybersecurity or security usability?

Demographic Questions

1. Gender: ∘ Male ∘ Female ∘ Other
2. Age: ∘ 18–20 ∘ 21–23 ∘ 24–26 ∘ >26
3. Which semester are you currently in? _____
4. Which department are you studying in? _____
5. How many years have you been using the Internet? _____
6. Do you play games? ∘ Yes ∘ No
7. If yes, what type of games do you usually play? _____
8. Have you ever played a learning-based game before? ∘ Yes ∘ No