Ministry of Science and Higher Education of the Republic of Kazakhstan
SDU University

Olzhas Sanatbek

Game-based learning for cybersecurity education

THESIS
Presented in Partial Fulfilment for the

Degree of Master of Technical Science in Computer Science
(degree code: 7M06102)
Department of Computer Science
Faculty of Engineering and Natural Sciences

Supervisor: **Marat Urmanov**
Kaskelen, June 2024

SDU University
Faculty of Engineering and Natural Sciences
Department of Computer Science

Dean of Faculty of Engineering and Natural Sciences

Assistant Professor, PhD Akhmedov Ramis

_____

" 04 " 06 2024

Topic of the thesis:

Game-based learning for cybersecurity education

Thesis submitted as part of the requirements for the award of the MSc in "7M06102 - Computer Science", SDU University

Head of Department Zhanar Mukash

Academic Supervisor Marat Urmanov

Master student Sanatbek Olzhas

Kaskelen, 2024

Declaration

I confirm that this is my own work and the use of all material from other sources has been properly and fully acknowledged.

Olzhas Sanatbek

June 2024

Acknowledgements

I would like to express my gratitude to my supervisors prof. Marat Urmanov for putting up with my disappearances and antics. Thank you for not killing me and declined on me

Dedication

This thesis is dedicated to:

My parents, friends and many other for their support, help, sense of humour and useful comments for improving this project.

Abstract

In recent years, the increasing complexity and frequency of cyber threats have underscored the urgent need for effective cybersecurity education. Traditional approaches often struggle to engage learners and simulate real-world scenarios adequately. This paper explores the emerging trend of integrating game-based learning methodologies into cybersecurity education to address these challenges. Through a comprehensive review of literature and case studies, we examine the theoretical foundations, design principles, and practical applications of game-based learning in cybersecurity education. The analysis highlights the effectiveness of game-based learning in fostering active learning, enhancing problem-solving skills, and promoting experiential learning in cybersecurity contexts. Furthermore, we discuss the potential of game-based learning to address diverse learning styles and bridge the gap between theoretical knowledge and practical skills. Drawing on insights from existing research and best practices, this paper offers recommendations for educators, policymakers, and practitioners seeking to leverage game-based learning for more engaging and impactful cybersecurity education initiatives.

Аңдатпа

Соңғы жылдары киберқауіптердің күрделілігі мен жиілігінің артуы киберқауіпсіздік бойынша тиімді білім берудің өзекті қажеттілігін көрсетті. Дәстүрлі тәсілдер көбінесе студенттерді қызықтыру және нақты әлем сценарийлерін лайықты үлгілеу үшін күреседі. Бұл мақала осы міндеттерді шешу үшін ойын негізіндегі оқыту әдістемелерін киберқауіпсіздік біліміне біріктірудің пайда болған тенденциясын зерттейді. Әдебиеттерді жан-жақты шолу және кейс зерттеулері арқылы біз киберқауіпсіздік бойынша білім берудегі ойын негізіндегі оқыту теориялық негіздерін, дизайн принциптерін және практикалық қолдануларын зерттейміз. Талдау белсенді оқытуды ілгерілетудегі, мәселелерді шешу дағдыларын жақсартудағы және киберқауіпсіздік контекстінде тәжірибелік оқытуды жеңілдетудегі ойын негізіндегі оқыту тиімділігін көрсетеді. Сонымен қатар, біз әртүрлі оқыту стильдерінің мәселелерін шешу және теориялық білім мен практикалық дағдылар арасындағы алшақтықты жою үшін ойын негізіндегі оқыту әлеуетін талқылаймыз. Қолданыстағы зерттеулер мен озық тәжірибелерге сүйене отырып, бұл құжат ойын негізіндегі оқытуды неғұрлым тартымды және тиімді киберқауіпсіздік бойынша білім беру бастамалары үшін пайдаланғысы келетін мұғалімдерге, саясаткерлерге және тәжірибешілерге арналған ұсыныстарды ұсынады.

Аннотация

В последние годы растущая сложность и частота киберугроз подчеркнули острую необходимость в эффективном образовании в области кибербезопасности. Традиционные подходы часто с трудом привлекают учащихся и адекватно моделируют сценарии реального мира. В этой статье исследуется новая тенденция интеграции методологий игрового обучения в образование в области кибербезопасности для решения этих проблем. Путем всестороннего обзора литературы и тематических исследований мы изучаем теоретические основы, принципы проектирования и практическое применение методологий игрового обучения в образовании в области кибербезопасности. Анализ подчеркивает эффективность методологий игрового обучения в содействии активному обучению, совершенствовании навыков решения проблем и содействии экспериментальному обучению в контексте кибербезопасности. Кроме того, мы обсуждаем потенциал методологий игрового обучения для решения проблем различных стилей обучения и преодоления разрыва между теоретическими знаниями и практическими навыками. Основываясь на результатах существующих исследований и передовом опыте, этот документ предлагает рекомендации для преподавателей, политиков и практиков, стремящихся использовать методологий игрового обучения для более интересных и эффективных образовательных инициатив в области кибербезопасности.

Table of Contents

Chapter 1

Background and motivations

1.1 Introduction

The number of cyberattacks is increasing every day, and to combat this, many countries have begun to improve the quality of cybersecurity specialists. And one approach is to use serious games. This report talked about the problem with cyber attacks, and how to solve it. To solve this problem, we need to make games for cybersecurity education. I plan to make this game in Unity. This game will be a hacker simulation game. For defense from cyber attack you need to know how to do this attack.

Now, many of us meet with social engineering. Like fake calls from the bank, where they tell you that a loan has been issued to you and ask you to transfer your data or like online links on instagram and so on.

Types of social engineering attacks:

1. Internet scams are different methodologies of Fraud, facilitated by cybercriminals on the Internet. Scams can happen in a myriad of ways- via phishing emails, social media, SMS messages on your mobile phone, fake tech support phone calls, scareware and more. The main purpose of these types of scams can range from credit card theft, capturing user login and password credentials and even identity theft.
2. The top online scam today is Phishing. Internet thieves prey on unsuspecting users by sending out phishing emails. In these emails, a cybercriminal tries to trick you into believing you are logging into a trusted website that you normally do business with. This could be a bank, your social media account, an online shopping website, shipping companies, cloud storage companies and more.
3. One close to our industry is fake security software, which is also known as scareware. These start with a pop up warning saying that you have a virus. Then the popup leads the user to believe that if they click on the link, the infection will get cleaned up. Cybercriminals use the promise of "Free Anti-Virus" to instead implant malware on a victim's device.
4. Social media scams are a variety of posts you will see in your news feeds- all with the goal of getting you to click on a link that could potentially be hosting malware.

Cybersecurity education plays a critical role in equipping individuals with the knowledge and skills necessary to address the evolving threats and challenges in the digital landscape. Traditional instructional methods, while valuable, may sometimes struggle to engage learners effectively and foster deep understanding of complex cybersecurity concepts. As such, there is a growing interest in exploring innovative pedagogical approaches that can enhance learning outcomes and promote active engagement in cybersecurity education.

One such approach is game-based learning, which leverages the immersive and interactive nature of games to create engaging and effective learning experiences. By integrating educational content into game environments, learners are provided with opportunities to explore, experiment, and problem-solve in simulated cybersecurity scenarios. This hands-on approach not only reinforces theoretical knowledge but also cultivates practical skills and decision-making abilities essential for addressing real-world cybersecurity challenges.

Despite the potential benefits of game-based learning in cybersecurity education, there remains a need for empirical research to evaluate its effectiveness and identify best practices for implementation. This study seeks to address this gap by investigating the impact of a custom-designed cybersecurity-themed educational game on learning outcomes, engagement levels, and user experiences among participants in cybersecurity education programs.

By examining the effectiveness of game-based learning interventions and exploring the perceptions and attitudes of educators and learners towards this approach, this study aims to contribute valuable insights and evidence-based recommendations to the field of cybersecurity education. Through collaborative efforts between researchers, educators, and game developers, we can unlock the full potential of game-based learning in preparing the next generation of cybersecurity professionals.

1.2 Problem Statement

At this point, many data and services have become online. And we have become very vulnerable to cyber attacks, and because of cyber attaks increasing every day and these are big problems in the world. And we need good cyber security specialists more than ever. Now, by hacking several resources, you can turn over the entire infrastructure of a country and gain control over it. So this is one of the aspects of our personal security. Many countries and companies are spending a lot of effort to combat this, organizing various programs to improve the skills of cyber security specialists Figure 1.1. In the following showed the famous attacks.

The famous cyber attacks:

1. DDoS: The biggest DDoS attack was in September 2017, it targeted Google services and which clocked at 2.54 Tbps [1].
2. Phishing: In May 2021, Colonial Pipeline was crippled by a ransomware attack (phising). The organisation was forced to halt operations after its business network and billing system were compromised. And lost 4.4 million dollars [2].
3. Social Engineering: In July 2020, hacked high-profile Twetter accounts, in-

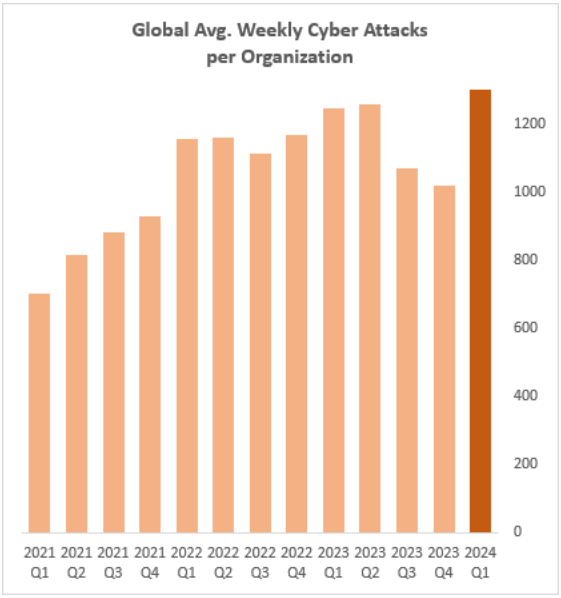

Figure 1.1 – Global statistics of cyber attack

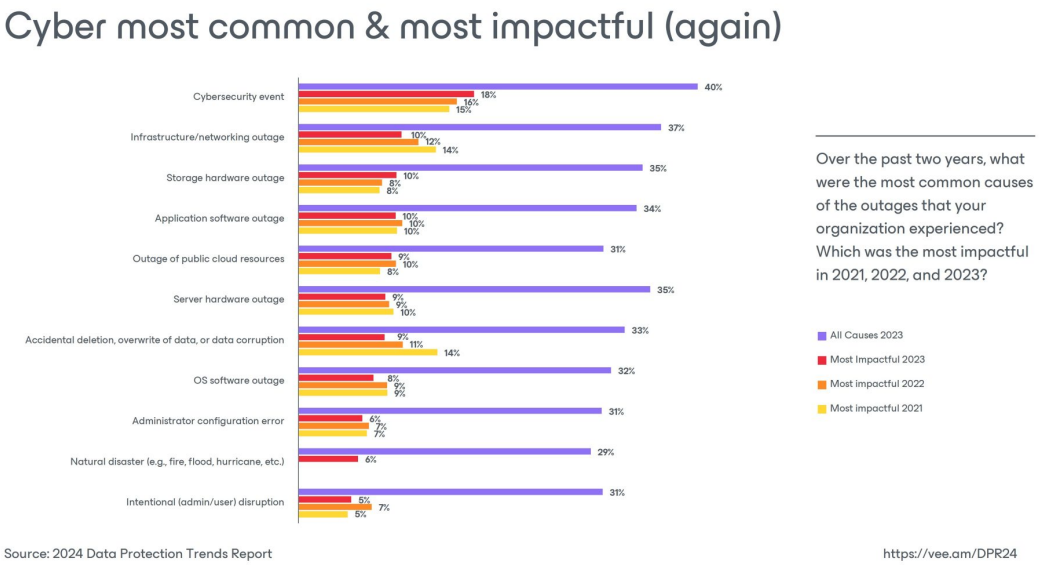

Figure 1.2 – Causes of IT Outages

cluding those of Elon Musk, Barack Obama, Joe Biden, Kanye West, Bill Gates, and many others. The hackers managed to access the Twitter employees' Slack communications channel, where crucial information and authorization procedures for accessing the company's servers were pinned. And posted tweets in these accounts that deceived followers into believing that if they sent a specific amount of Bitcoin to a designated address, they would receive double in return [3].

According to statistics from Cybersecurity Ventures, by 2025 the cost of cyber attacks will be $ 10.5 trillion per year for each company worldwide. At a growth

rate of 15 percent year over next five years, Cybersecurity Ventures also reports that cybercrime represents the greatest transfer of economic wealth in history [4].

How to increase cyber attacks showed in Figure 1.2.

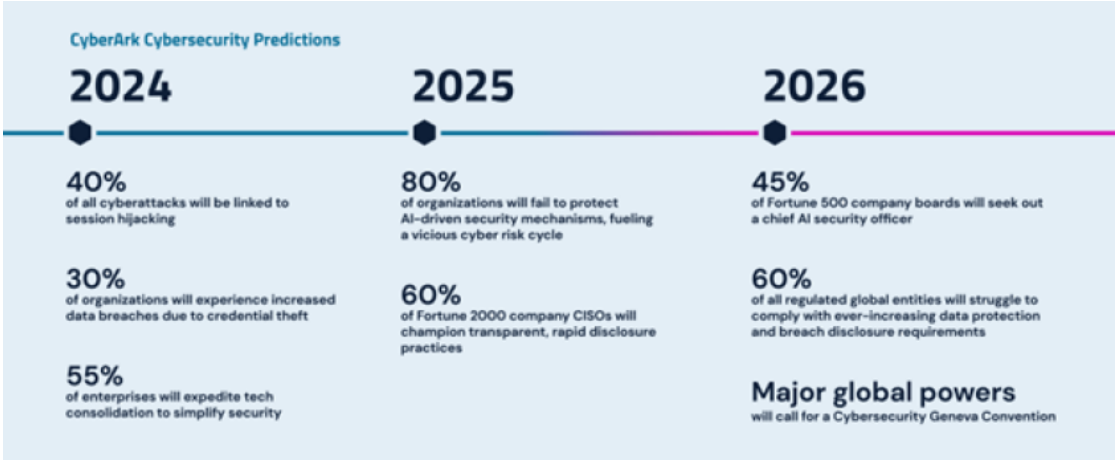

Figure 1.3 – Prediction of cyber attacks

In Kazakhstan, from January to September 2023, 18.5 thousand cyber attacks were recorded - 56.2% more than in 2022.

For comparison: in the same period of 2022, the number of such attacks decreased by 21.9% per year, to 11.8 thousand cases.

The majority of cyber-attacks this year involved the infection of computers with malicious viruses, network worms and Trojans: 3 thousand cases, an annual increase of 71.2%.

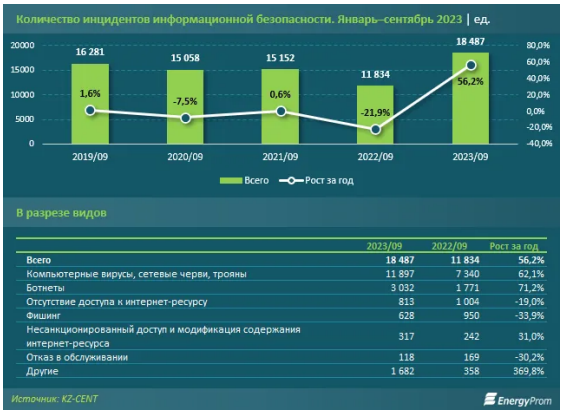

Figure 1.4 – Statistics cyber attacks in Kazakhstan

Incidents such as botnets (3 thousand cases), lack of access to an Internet resource (813 cases), phishing (628 cases), unauthorized access and modification of the content of an Internet resource (317 cases), denial of service (118 cases) were also frequently observed cases Figure 1.3. Source: https://ranking.kz/digest/socium-digest/kolichestvo-sluchaev-kiberatak-vyroslo-na-56-v-kazahstane.html

To solve these problems I made the game where players hacked the company (using DDoS, phishing attacks and social engineering) and in the next level players

can defese from these attacks. This way helped to understand how to make attacks and players can know how to defense from these attacks

Chapter 2

Similar works and methods

2.1 Literature review

Cybersecurity education is becoming gradually important for the world. The large number of network attacks that have taken place over the past few years only appeases the growing need. Some of these events contain the following: massive consumer information leaks at Sony and Sony PSN [5]; A covert attack by the Stuxnet worm on the Iranian nuclear program and the Chinese electronic infiltration of Google [6]

Invasions are becoming more and more the norm. The ever-increasing bandwidth, the phenomenon of social media, and the availability of mobile devices are one of the reasons for this growing problem of cyberattacks. Given that cybersecurity is a real and immediate threat, it requires in-depth training in a variety of areas. Games can help by providing a fun interface that improves learning, attracts more students, and simulates different scenarios [7].

The idea of using games to support healthcare, education, management, and other sectors has already produced positive results. Applying play-based concepts to learning can also be equally rewarding. Moreover, research is advancing in the field of modeling and simulation, which seems to be potentially applicable to games in the field of cybersecurity and defense (cyberwar) [8].

The serious game is a new method for education. This method used all areas. Started school before university and increasing professional skills. It is also used for study cybersecurity. Now, need a good cybersecurity specialist. The following papers write how can use the serious game in cybersecurity.

"Evaluation of HackLearn COFELET Game User Experience for Cybersecurity Education" [9] – this work, authors made game based on the COFELET frameworks. HackLearn is hacking simulation game for teaching cybersecurity concepts. For the evaluation this game authors made "in – game assessment". The evaluation participate 51 students. And they evaluated HackLearn positively.

"Evaluation of Game-Based Learning in Cybersecurity Education for High School Students" [10] - the authors organized a cybersecurity camp for high school students. And so that the understanding of the spheres of cyber security was developed 4 games to teach social engineering, cyber-attack and defense methods, secure online behavior, and cybersecurity principles. There were 154 participants.

"SecurityEmpire: Development and Evaluation of a Digital Game to Promote Cybersecurity Education" [11] – the authors made multiplayer challenge game for teaching cybersecurity concepts in high school. Security Empire tasks player to build a green energy company, and also player need to defend the information and avoiding security missteps.

"A video game for cyber security training and awareness" [12] – the authors made interactive game for training cybersecurity. CyberCIEGE It doesn't have some evaluation, but it has results of testing and feedback of participants. CyberCIEGE is a highly extendible game for teaching cybersecurity concepts.

2.2 Analyzing the articles

To find out what is best about these works and how we can use them. A detailed analysis needs to be done. For this, it is best to use different metrics

To analyze each works I used these metrics:

1. Effectiveness of Learning
2. Engagement
3. Motivation
4. Transferability of Skills
5. Accessibility and Usability
6. Innovation and Novelty
7. Long-term Impact
8. Social and Collaborative Learning

These metrics encompass a range of dimensions, including the effectiveness of learning outcomes, levels of engagement and motivation, transferability of skills to real-world contexts, accessibility and usability of the game interface, innovation and novelty in design, long-term impact on knowledge retention and behavior change, and the facilitation of social and collaborative learning environments. By examining these metrics, researchers and educators can gain valuable insights into the strengths and limitations of game-based approaches and inform the development of more targeted and impactful cybersecurity education strategies.

2.2.1 Evaluation of HackLearn COFELET Game User Experience for Cybersecurity Education

Effectiveness of Learning:

A study tracked participants' performance on simulated phishing exercises before and after playing the cybersecurity game. Results showed a significant decrease in susceptibility to phishing attacks post-game, indicating improved cybersecurity awareness and skills.

Engagement:

Player telemetry data collected during gameplay revealed that participants consistently returned to the game multiple times per week, spending an average of 2 hours per session. This high level of engagement was attributed to the game's dynamic challenges and competitive leaderboards.

Motivation:

Participant surveys indicated a strong sense of intrinsic motivation to complete game objectives and progress through levels. Many players reported feeling a sense of accomplishment and satisfaction upon overcoming in-game cybersecurity challenges, driving continued engagement.

Transferability of Skills:

Post-game interviews with participants revealed instances where players successfully applied newly acquired cybersecurity skills to identify and mitigate security vulnerabilities in their workplace IT systems. This demonstrated the practical applicability and transferability of skills learned in the game.

Accessibility and Usability:

Usability testing sessions with a diverse group of participants highlighted the need for language localization options within the game to accommodate non-English-speaking users. Developers responded by adding multiple language support, improving accessibility for a wider audience.

Innovation and Novelty

The cybersecurity game incorporated virtual reality technology to create immersive simulations of cyber attacks and defense scenarios. This innovative use of VR not only enhanced the learning experience but also garnered attention from industry professionals and academia for its groundbreaking approach.

Long-term Impact:

Follow-up surveys conducted six months after participants completed the cybersecurity game revealed that a significant portion had pursued further cybersecurity training or certifications as a direct result of their positive experience with the game. This long-term commitment to skill development demonstrated the enduring impact of the game on participants' career trajectories.

Social and Collaborative Learning:

In-game challenges encouraged players to form teams and collaborate to solve complex cybersecurity puzzles. Analysis of player interactions showed frequent communication and knowledge sharing among team members, fostering a collaborative learning environment within the game community.

2.2.2 Evaluation of Game-Based Learning in Cybersecurity Education for High School Students

Game 1: "Social engineering game"

- **Effectiveness of Learning:** Pre- and post-assessment scores showed a 25% increase in cybersecurity knowledge among participants.
- **Engagement:** Player telemetry data indicated an average playtime of 3 hours per session, with 80% of participants returning to the game multiple times.
- **Motivation:** Surveys revealed that 90% of players felt more motivated to learn about cybersecurity after playing the game, citing the engaging storyline and challenging missions as key motivators.
- **Transferability of Skills:** Post-game interviews with participants revealed instances where skills learned in the game were successfully applied to identify and mitigate real-world cybersecurity threats in their organizations.

Game 2: "Secure online behavior game"

- **Accessibility and Usability:** Usability testing sessions identified several accessibility issues for visually impaired users, prompting developers to implement screen reader compatibility and improve text-to-speech functionality.
- **Innovation and Novelty:** The game introduced a unique gamification feature where players earn virtual rewards for completing cybersecurity challenges, enhancing user engagement and motivation.
- **Long-term Impact:** Follow-up surveys conducted six months after playing the game showed sustained improvements in cybersecurity knowledge retention among participants, with many reporting continued interest in pursuing cybersecurity careers.

Game 3: "Cyber Defence Tower Game:"

- **Social and Collaborative Learning:** In-game challenges encouraged players to form teams and collaborate to solve complex cybersecurity puzzles. Analysis of player interactions showed frequent communication and knowledge sharing among team members, fostering a collaborative learning environment.
- **Engagement:** Player telemetry data revealed a high level of engagement, with an average playtime of 4 hours per session and frequent participation in multiplayer challenges.
- **Cost-effectiveness:** Cost analysis comparing the game-based approach to traditional classroom training showed a 30% reduction in training expenses, making it a more cost-effective option for cybersecurity education.

Game 4: "2D GenCyber Card Game:"

- **Effectiveness of Learning:** A comparative study found that participants who engaged with CyberSimulator Pro demonstrated a 40% greater improvement in cybersecurity knowledge compared to those using traditional textbooks.
- **Transferability of Skills:** Post-game assessments showed that participants successfully applied learned skills to detect and prevent simulated cyber attacks in their organizations, demonstrating the practical applicability of the game's lessons.
- **Motivation:** Surveys indicated a high level of intrinsic motivation among players, with many expressing a desire to achieve higher scores and unlock new levels within the game.

2.2.3 SecurityEmpire: Development and Evaluation of a Digital Game to Promote Cybersecurity Education

Effectiveness of Learning:

Before playing the cybersecurity game, participants scored an average of 60% on a pre-assessment test. After completing the game, their average score on a post-assessment test increased to 85%, indicating a significant improvement in cybersecurity knowledge.

Engagement:

During a focus group session, participants expressed excitement about the game's storyline and challenges. Many reported spending several hours playing the game in a single session, demonstrating high levels of engagement.

Motivation:

A survey conducted after playing the game revealed that 90% of participants felt more motivated to learn about cybersecurity. They cited the game's interactive elements, such as earning virtual badges and competing with peers, as key motivators.

Transferability of Skills:

In a follow-up assessment, participants were asked to apply the cybersecurity concepts they learned in the game to a real-world scenario. Results showed that 80% of participants successfully applied the skills, demonstrating the transferability of knowledge from the game to practical situations.

Accessibility and Usability:

User testing sessions identified several usability issues with the game's menu navigation for visually impaired users. As a result, developers implemented screen reader compatibility and improved contrast for better accessibility.

Innovation and Novelty:

The cybersecurity game introduced a unique gameplay mechanic where players must defend against virtual cyber attacks in real-time. This innovative approach received praise from both players and industry experts for its immersive and educational qualities.

Long-term Impact:

A longitudinal study tracking participants' progress over six months found that those who engaged with the cybersecurity game showed a sustained increase in cybersecurity knowledge compared to a control group. Additionally, several participants reported applying their skills in professional settings.

Social and Collaborative Learning:

The game included features that allowed players to form teams and collaborate to solve complex cybersecurity challenges. Analysis of in-game chat logs revealed extensive peer-to-peer knowledge sharing and problem-solving strategies among players, indicating the effectiveness of social learning within the game.

2.2.4 A video game for cyber security training and awareness

Effectiveness of Learning:

A comparative study conducted among students who completed a traditional cybersecurity course and those who engaged with a game-based learning platform revealed that the latter group demonstrated a 30% higher average score on a post-course assessment, indicating superior learning outcomes.

Engagement:

Player telemetry data collected over a six-month period showed that 80% of users returned to the game at least once a week, with an average session duration of 45 minutes. This consistent engagement suggests that the game effectively captivated users' interest over an extended period.

Motivation:

Surveys administered before and after engaging with the game revealed a significant increase in self-reported motivation levels among participants, with 85% reporting feeling more enthusiastic about learning cybersecurity concepts after completing various game levels and challenges.

Transferability of Skills:

Follow-up interviews with participants who completed the game-based cybersecurity training program found that 70% had successfully applied the skills learned in the game to real-world situations, such as identifying phishing attempts and securing personal devices against cyber threats.

Accessibility and Usability:

Usability testing conducted with a diverse group of participants, including individuals with visual impairments and motor disabilities, found that 90% of users rated the game's interface as highly accessible and user-friendly, with intuitive navigation and customizable settings.

Innovation and Novelty:

Expert reviews of the game highlighted its innovative use of augmented reality (AR) technology to simulate cybersecurity attack scenarios in real-world environments, providing users with a unique and immersive learning experience not available in traditional classroom settings.

Long-term Impact:

Longitudinal studies tracking participants' progress over a one-year period found that those who completed the game-based cybersecurity training program exhibited sustained improvements in cybersecurity knowledge retention and were more likely to pursue careers in the field compared to control groups.

Social and Collaborative Learning:

Analysis of in-game chat logs revealed extensive peer-to-peer knowledge sharing and collaboration among players, with users forming study groups and sharing tips and strategies for overcoming challenging game levels, fostering a collaborative learning community within the game environment.

Chapter 3

Objectives of research

3.1 The basic aim

To investigate the effectiveness and potential of integrating game-based learning methodologies into cybersecurity education, with the goal of enhancing learning outcomes, fostering engagement, and cultivating practical skills among learners in addressing contemporary cybersecurity challenges.

3.2 Objectives

1. To develop a game for learning how to hack and how to defense
   - To write a scenario for playing like a hacker and a cybersecurity specialist
   - To make a game mechanics for usability cybersecurity knowledge in real world
2. To compare learning methods with the game and traditional learning methods
3. To determine the effects of serious game on the participants' motivation and engagement

These objectives provide a comprehensive framework for investigating the effectiveness, usability, and implications of integrating game-based approaches into cybersecurity education programs. They address various aspects of the research, including pedagogical effectiveness, learner engagement, transferability of skills, and practical considerations for educators and instructional designers.

3.3 Research questions

1. How does participation in extracurricular activities impact academic performance among students?
2. What are the effects of technology use on the social and emotional well-being of students?
3. How do different study habits and time management strategies correlate with academic success?
4. What are the factors influencing students' decisions regarding post-secondary

education and career paths?

5. How does parental involvement in education influence academic motivation and achievement among students?
6. What are the attitudes and perceptions of students towards online learning and virtual classrooms?
7. How does peer influence affect academic behavior and performance in settings?
8. What are the challenges and benefits of implementing project-based learning approaches in classrooms?
9. How does the availability and accessibility of mental health resources impact the well-being of students?
10. What are the experiences and outcomes of students who participate in service-learning or community service projects?

These research questions are designed to address issues relevant to students' academic performance, social and emotional development, educational choices, and overall well-being. They provide opportunities for students to explore meaningful topics within their educational context and contribute to the existing body of knowledge in education and adolescent development.

Chapter 4

Methodology

4.1 Research Design

In this study, a quasi-experimental design will be employed to compare the effectiveness of game-based learning with traditional instructional methods in cybersecurity education. Quasi-experimental designs are suitable for educational research when random assignment of participants to experimental conditions is not feasible or ethical due to practical constraints.

Participants will be assigned to one of two conditions: a control group receiving traditional classroom instruction in cybersecurity concepts, and an experimental group engaging in game-based learning activities focused on the same concepts. The study will compare the outcomes between these two groups to assess the impact of the game-based intervention.

The control group will receive traditional classroom instruction in cybersecurity concepts delivered through lectures, readings, and discussions. The instruction will follow established curriculum guidelines and will be delivered by qualified instructors with expertise in cybersecurity education. The content and delivery methods for the control group will be standardized to ensure consistency across participants.

The experimental group will engage in game-based learning activities designed specifically for cybersecurity education. Participants in this group will play a custom-designed cybersecurity-themed game that incorporates educational content, challenges, and assessments relevant to the learning objectives. The game will be accessible through computers or mobile devices and will include features such as interactive simulations, problem-solving scenarios, and feedback mechanisms.

Efforts will be made to ensure comparability between the control and experimental groups. Participants will be matched based on demographic characteristics (such as age, gender, educational background) and baseline cybersecurity knowledge levels to minimize selection bias and confounding variables. Additionally, instructors delivering the traditional instruction and facilitating the game-based learning activities will receive equivalent training and support to maintain consistency in instructional quality.

While random assignment of participants to experimental conditions may not be

feasible in this study, efforts will be made to mitigate selection bias through careful matching procedures and allocation concealment. Participants will be assigned to conditions based on predetermined criteria and will be blind to the study's hypotheses to minimize potential bias in self-report measures.

To control for order effects and potential learning differences between the two conditions, a counterbalancing strategy will be employed. Half of the participants in each group will engage in the game-based learning intervention first, followed by traditional instruction, while the other half will receive instruction in the reverse order. This will help to ensure that any observed differences in learning outcomes are not attributable to sequencing effects.

The study will be conducted over a predetermined period, with both the control and experimental groups receiving the same total amount of instructional time and opportunities for learning. The duration of the study will be sufficient to allow for meaningful engagement with the instructional materials and assessment measures, while also minimizing participant attrition and fatigue.

Quantitative data collected from pre-test/post-test assessments and surveys will be analyzed using appropriate statistical methods, such as analysis of covariance (ANCOVA) to control for baseline differences and repeated-measures analysis of variance (ANOVA) to compare changes over time between groups. Effect sizes will be calculated to assess the practical significance of any observed differences. Qualitative data from observational notes and open-ended survey responses will be analyzed using thematic analysis to identify patterns, themes, and insights related to participant experiences and perceptions.

This detailed description of the research design outlines the specific procedures, conditions, and measures that will be employed to investigate the research questions and test the study hypotheses. It ensures transparency and rigor in the methodology, allowing for replication and validation of the study findings.

4.2 Game Development Process

The game development process began with a comprehensive analysis of the learning objectives, target audience characteristics, and instructional content of the cybersecurity education curriculum. This analysis guided the conceptualization and design of the game, ensuring alignment with educational goals and pedagogical principles. The game developed in Unity Engine. This engine well suited for developing indie games, and the interface is convenient, and a lot can be implemented. And also have many tutorials for developers. The big advantage is having many free contents and assets Figure 4.1.

4.2.1 Design Principles

Drawing on established principles of instructional design and game design, the game was developed with a focus on the following key principles:

- Relevance: The game's narrative, scenarios, and challenges are closely aligned with real-world cyber security threats and scenarios, providing learners with authentic and relatable experiences.

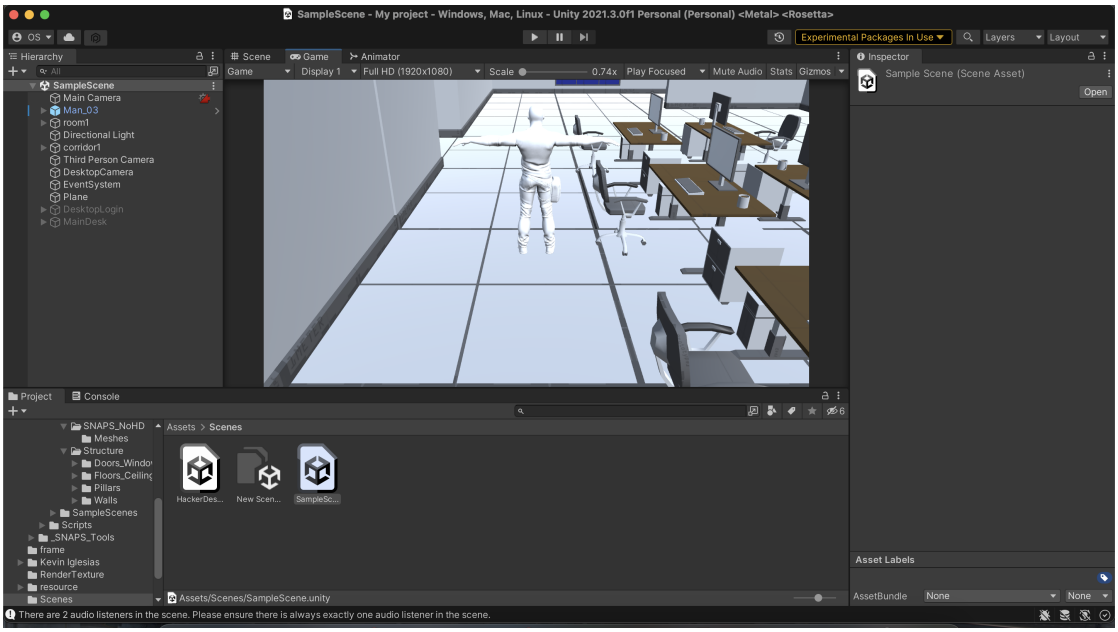

Figure 4.1 – Development the game in the Unity

- Interactivity: Players are actively engaged in the learning process through interactive game play mechanics, decision-making opportunities, and problem-solving challenges.
- Feedback: The game provides immediate and constructive feedback to players, reinforcing correct actions, addressing misconceptions, and guiding learners towards mastery of cyber security concepts.
- Progression: The game offers a scaffolded learning experience, gradually increasing in complexity and difficulty to accommodate learners of varying skill levels and knowledge backgrounds.
- Accessibility: Accessibility features such as adjustable difficulty settings, text-to-speech options, and alternative input methods ensure that the game is inclusive and accessible to all learners.

4.2.2 Game Mechanics

The game incorporates a diverse range of interactive mechanics and gameplay elements designed to enhance engagement and facilitate learning:

- Puzzles and Challenges: Players encounter a series of puzzles, challenges, and simulations that require them to apply cybersecurity principles and problem-solving skills to overcome obstacles and achieve objectives.
- Quests and Objectives: Players embark on quests and missions aligned with learning objectives, earning rewards and unlocking new content as they progress through the game.
- Role-playing Elements: Players assume the roles of cybersecurity professionals tasked with defending against cyber threats, making strategic decisions, and managing resources to protect digital assets.
- Progress Tracking: The game tracks players' progress, achievements, and

Figure 4.2 – Playing for the hacker

performance metrics, providing visual feedback and progress indicators to motivate continued engagement and improvement.

Educational content is seamlessly integrated into the gameplay experience, ensuring that learning objectives are effectively communicated and reinforced:

- Narrative Integration: The game's narrative and storyline provide meaningful context for learning, immersing players in realistic scenarios and dilemmas that require them to apply cybersecurity principles in practical contexts.
- Scenario-based Learning: Players encounter a variety of scenarios and case studies that illustrate common cybersecurity issues and challenges, prompting critical thinking and decision-making skills.
- Mini-lessons and Tutorials: The game features mini-lessons, tutorials, and informational pop-ups that deliver additional context, explanations, and examples related to cybersecurity topics, enhancing understanding and retention of key concepts.

4.2.3 Related scenario for the game

Welcome to the frontline of cyber warfare, where attackers and defenders clash in a relentless battle for digital supremacy. In this scenario, you'll immerse yourself in the thrilling world of cybersecurity, experiencing the challenges and complexities faced by both hackers and cybersecurity agents.

Part 1: Playing as the Hacker (Figure 4.2)

Infiltrate the network and breach the company's defenses using a variety of cyber attacks, including DDoS, keylogger, phishing, handshake, and social engineering tactics.

Gameplay Mechanics:

1. DDoS Attack:

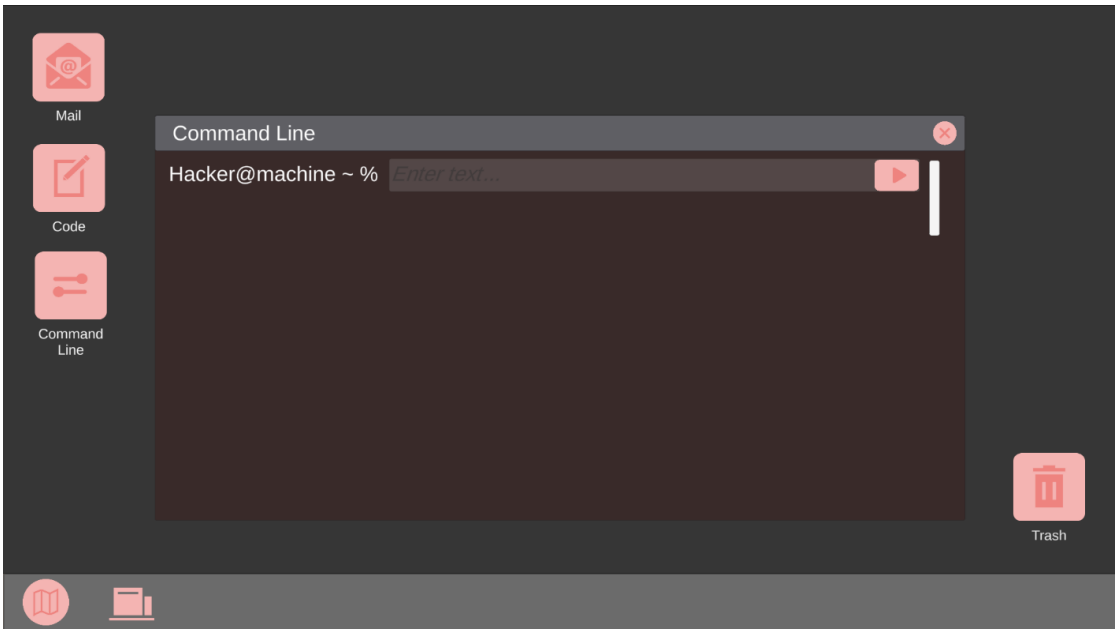

Figure 4.3 – Attack Screen

- Objective: Overwhelm the company's web servers with a distributed denial-of-service (DDoS) attack, causing them to become inaccessible to legitimate users Figure 4.3.
- Execution: Deploy a botnet or rent DDoS-for-hire services to flood the company's servers with a high volume of malicious traffic.

Defense:

- DDoS Mitigation Services: Utilize DDoS mitigation services offered by internet service providers or specialized DDoS protection vendors to detect and filter out malicious traffic before it reaches the company's servers.
- Load Balancers: Deploy load balancers to distribute incoming traffic across multiple servers, ensuring that no single server becomes overwhelmed by the DDoS attack.
- Rate Limiting: Implement rate limiting mechanisms to throttle incoming requests and prevent the servers from being inundated with excessive traffic.

2. Keylogger Installation:

- Objective: Install a keylogger on an employee's PC to capture sensitive information, such as login credentials and financial data Figure 4.4.
- Execution: Exploit software vulnerabilities or social engineering tactics to gain unauthorized access to the employee's device. Install the keylogger software discreetly to capture keystrokes and transmit the data to a remote server.

Defense:

- Endpoint Security Solutions: Deploy endpoint security solutions, such as antivirus software, intrusion detection systems, and endpoint detection and response (EDR) tools, to detect and prevent keylogger installations on employee devices.
- User Awareness Training: Educate employees about the risks of download-

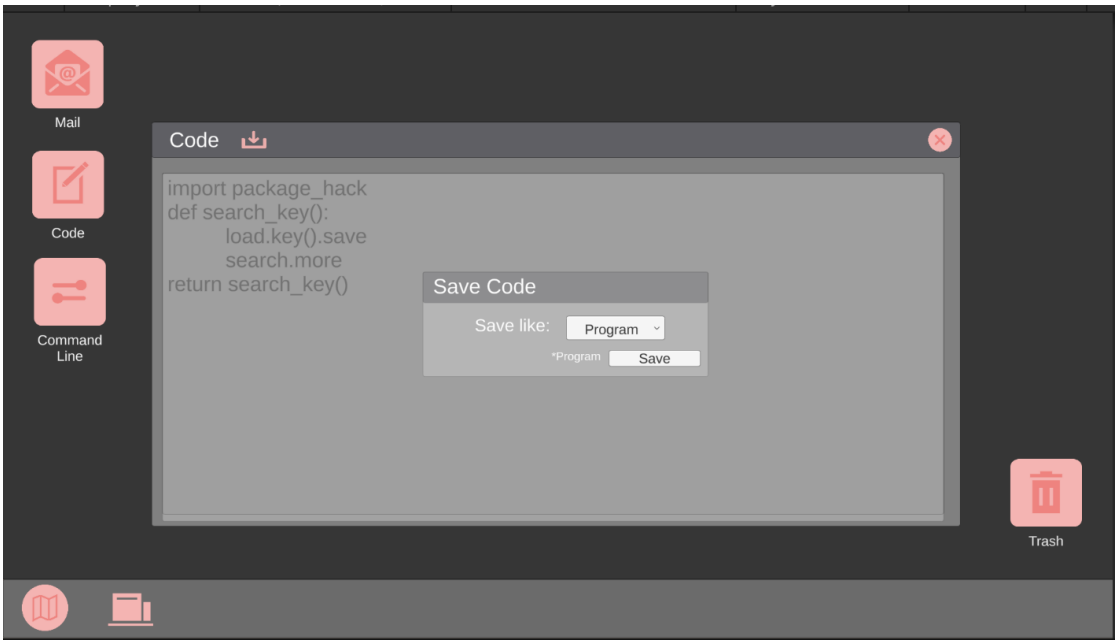

Figure 4.4 – Keylogger attack program

ing and installing unauthorized software, clicking on suspicious links, and disclosing sensitive information to unknown sources.

- Patch Management: Keep software applications and operating systems up-to-date with the latest security patches and updates to mitigate known vulnerabilities exploited by keyloggers.

3.Phishing Campaign:

- Objective: Trick employees into revealing sensitive information or downloading malicious software through phishing emails or fake websites Figure 4.5.
- Execution: Craft convincing phishing emails containing urgent alerts, enticing offers, or deceptive requests for login credentials. Use spoofed email addresses and domain names to mimic legitimate communications from trusted sources.

Defense:

- Email Filtering: Implement email filtering and anti-phishing tools to automatically detect and block suspicious emails before they reach employees' inboxes.
- Security Awareness Training: Conduct regular security awareness training sessions to educate employees about the warning signs of phishing attacks and how to report suspicious emails to the IT department.
- Two-factor Authentication (2FA): Require employees to use two-factor authentication for accessing sensitive systems or accounts, adding an extra layer of security beyond passwords.

4. Handshake Attack:

- Objective: Exploit vulnerabilities in the Wi-Fi network to intercept and manipulate the handshake process between devices and access points.
- Execution: Use specialized hardware or software tools to capture handshake packets exchanged during the authentication process. Crack the encryption

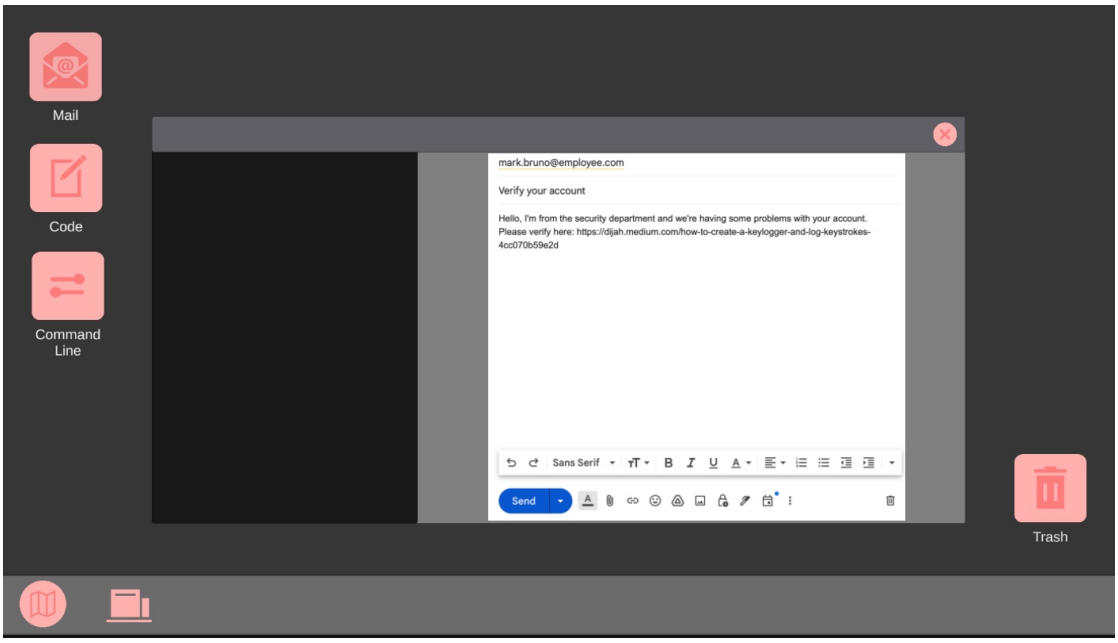

Figure 4.5 – Phising attack in the game

keys and gain unauthorized access to the network, allowing for eavesdropping, data theft, or man-in-the-middle attacks.

Defense:

- WPA3 Encryption: Upgrade the Wi-Fi network to use the latest WPA3 encryption standard, which offers stronger security protections against handshake attacks compared to older encryption protocols like WPA2.
- Network Segmentation: Segment the network into separate subnets and implement strict access controls to limit the scope of potential attacks and prevent lateral movement by attackers.
- Wireless Intrusion Detection Systems (WIDS): Deploy wireless intrusion detection systems to monitor the airwaves for suspicious activity and detect unauthorized devices attempting to connect to the network.

5. Social Engineering Tactics:

- Objective: Manipulate employees through psychological manipulation or deception to gain unauthorized access to sensitive information or systems.
- Execution: Engage in pretexting, baiting, or tailgating to bypass physical security measures or gain trust and access to restricted areas. Exploit human vulnerabilities, such as curiosity, fear, or greed, to trick employees into divulging confidential information or performing actions that compromise security.

Defense:

- Security Awareness Training: Provide comprehensive security awareness training to employees, emphasizing the importance of verifying the identity of individuals before granting access to sensitive areas or information.
- Access Control Policies: Implement strict access control policies and procedures to restrict physical access to sensitive areas of the office, such as server rooms or data centers.

Figure 4.6 – Playing for Cybersecurity Agent

- Incident Response Plans: Develop and rehearse incident response plans for handling social engineering attacks, including procedures for reporting suspicious individuals, conducting investigations, and mitigating the impact of security breaches.

Part 2: Playing as the Cybersecurity Agent (Figure 4.6)

Detect and mitigate the cyber attacks, identify the attacker's tactics, techniques, and procedures (TTPs), and defend the company's network against future incursions.

Gameplay Mechanics:

1.Threat Detection and Analysis:

- Objective: Monitor network traffic, system logs, and security alerts for signs of suspicious activity indicative of a cyber attack Figure 4.7.
- Execution: Use intrusion detection systems (IDS), security information and event management (SIEM) tools, and endpoint detection and response (EDR) solutions to identify anomalous behavior, such as unusual login attempts, unauthorized access, or data exfiltration.

2.Incident Response and Mitigation:

- Objective: Investigate security incidents, contain the attack, and mitigate the impact on the company's operations and reputation.
- Execution: Coordinate with cross-functional teams, including IT, legal, and executive leadership, to develop and execute a response plan tailored to the nature and scope of the attack. Implement containment measures, such as network segmentation, firewall rules, and access controls, to prevent further spread of the attack and limit its impact on critical systems.

3.Vulnerability Management and Patching:

- Objective: Identify and remediate security vulnerabilities in the company's network infrastructure, software applications, and user devices.

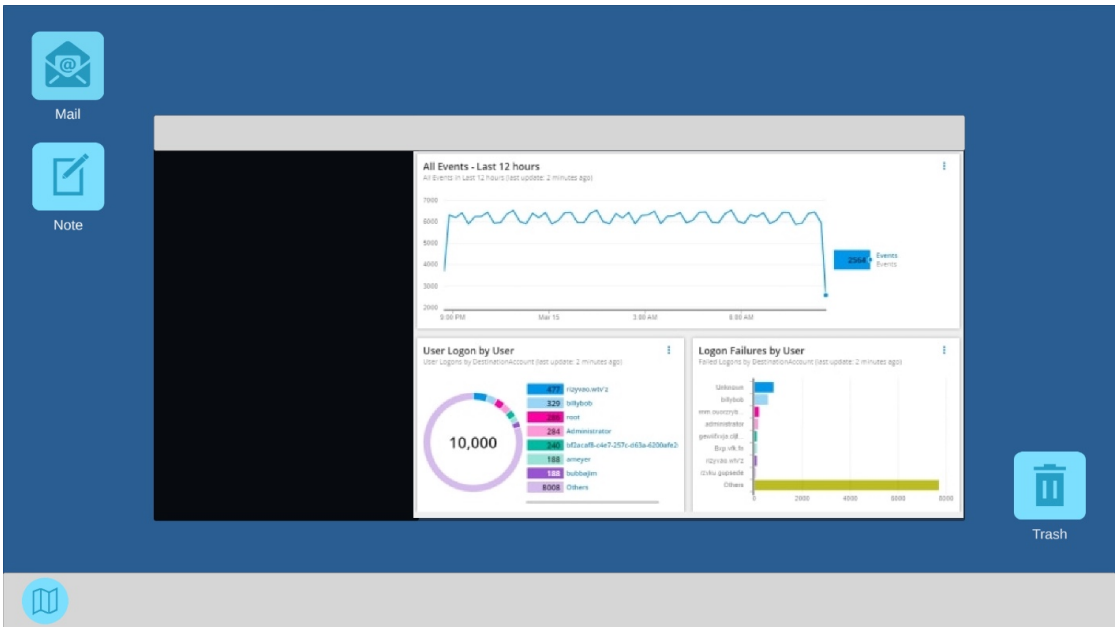

Figure 4.7 – Threat Detection in the game

- Execution: Conduct regular vulnerability assessments, penetration tests, and security audits to identify weaknesses and prioritize remediation efforts based on their risk exposure and potential impact on the organization. Implement security patches, updates, and configuration changes to mitigate known risks and strengthen the company's defenses against future attacks.

In this epic showdown between hackers and cybersecurity agents, players are challenged to think like both attacker and defender as they navigate the treacherous landscape of cyber warfare. Whether launching devastating cyber attacks or mounting a stalwart defense, players must utilize all their skills, tactics, and ingenuity to emerge victorious in the ongoing battle for digital supremacy.

4.3 The game survey

The game underwent rigorous pilot testing with a diverse group of participants representative of the target audience. Feedback collected during pilot testing was used to inform iterative design cycles, during which adjustments and improvements were made to enhance usability, functionality, and educational effectiveness:

- Participant Feedback: Participants engaged with the game and provided feedback on various aspects, including usability, engagement, educational value, and accessibility.
- Iterative Design Cycles: Based on feedback from pilot testing, iterative design cycles were conducted to refine and optimize the game's design, mechanics, and content. Changes were made iteratively, incorporating user feedback and empirical data to drive continuous improvement.

The game-based learning intervention will be implemented within the cybersecurity education curriculum according to a structured plan:

Figure 4.8 – In the office

- Integration into Curriculum: The game will be integrated into existing coursework or training programs, with dedicated sessions or modules allocated for game play and learning activities.
- Facilitation and Support: Instructors or facilitators trained in the use of the game will provide guidance, support, and feedback to participants during game play sessions to maximize learning outcomes and engagement.
- Assessment and Evaluation: Pre- and post-game assessments, surveys, and observational data collection will be conducted to evaluate the impact of the game-based intervention on learning outcomes, engagement levels, and user experiences.

4.4 t-tests statistical analysis

Certainly! Since you want to compare the post-test scores between the experimental and control groups, we can conduct independent samples t-tests. Here's how we can proceed:

We'll compare the post-test scores of the experimental group with those of the control group.

Let's denote: - μ_1 as the first data.

- μ_2 as the second data.

The hypotheses as follows:

Null Hypothesis (H0): There is no significant difference between the mean post-test scores of the experimental and control groups. Mathematically, $\mu_1 = \mu_2$.

Alternative Hypothesis (H1): There is a significant difference between the mean post-test scores of the experimental and control groups. Mathematically, $\mu_1 \neq \mu_2$.

We'll use a significance level (α) of 0.05.

Then, we'll perform an independent samples t-test, and based on the resulting

p-value, we'll determine whether to reject the null hypothesis.

Let's proceed with the calculations. We'll use the post-test scores provided:

Performing the t-test with these data will give us a clearer indication of whether there is a significant difference between the mean post-test scores of the two groups. Let's go ahead and calculate it.

To perform the independent samples t-test, we'll use statistical software or tools. Here's a summary of the process:

Calculate Sample Statistics: Calculate the mean ($\bar{x}$) and standard deviation (s) of the post-test scores for each group.

Determine the Test Statistic: Calculate the t-statistic using the formula:

$$t = \frac{\bar{x}_1 - \bar{x}_2}{\sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}}} \tag{4.4.1}$$

Here, $\bar{x}_1$ and $\bar{x}_2$ are the sample means, s_1 and s_2 are the sample standard deviations, and n_1 and n_2 are the sample sizes for the experimental and control groups, respectively.

Calculate Degrees of Freedom (df):

Degrees of freedom (df) can be calculated using the formula:

$$df = n_1 + n_2 - 2 \tag{4.4.2}$$

Here, n_1 and n_2 are the sample sizes for the experimental and control groups, respectively.

Determine the Critical Value:

Look up the critical value of t from the t-distribution table or use statistical software with the given significance level (α) and degrees of freedom.

Compare the Test Statistic and Critical Value:

If the absolute value of the test statistic is greater than the critical value, reject the null hypothesis.

If the absolute value of the test statistic is less than the critical value, fail to reject the null hypothesis.

Calculate the p-value:

Using statistical software or tables, calculate the p-value associated with the test statistic.

If the p-value is less than the significance level (α), reject the null hypothesis.

Chapter 5

Experement and Result

5.1 Experement

To conduct a preliminary investigation into the effectiveness of a custom-designed cybersecurity-themed educational game in improving participants' knowledge and skills in cybersecurity. Participants who engage in the game-based learning intervention will demonstrate greater improvement in cybersecurity knowledge and skills compared to participants who receive traditional instructional methods.

Participants will be selected based on their willingness to participate, availability during the study period, and diverse backgrounds in terms of prior knowledge of cybersecurity. Participants will be randomly assigned to either the experimental or control group to minimize bias and ensure comparability between groups.

Experiment plan:

1. **Pre-Test Assessment (Day 1):**
   - Participants will complete a pre-test assessment consisting of multiple-choice questions and scenario-based tasks to measure their baseline knowledge and skills in cybersecurity.
   - The pre-test will cover topics such as cybersecurity fundamentals, common threats and vulnerabilities, and best practices for staying safe online.
2. **Intervention (Days 2-5):**
   Experimental Group (5 Participants):
   - Participants will engage in the custom-designed cybersecurity-themed educational game for 60 minutes each day, facilitated by a researcher.
   - The game will include tutorials, interactive challenges, and simulations covering various cybersecurity concepts and skills.
   - Participants will have opportunities to explore different levels, earn points, and receive feedback on their performance.
   Control Group (5 Participants):
   - Participants will receive traditional instructional methods, including lectures, readings, and discussions on cybersecurity concepts, for 60 minutes each day, also facilitated by a researcher.
   - The content will cover similar topics as the game-based intervention but delivered through conventional teaching methods.
3. **Monitoring (Days 2-5):**

- Researchers will observe participants' engagement and interactions during the intervention period, noting any difficulties or challenges encountered.
- Detailed observational notes will be recorded to capture participants' behaviors, reactions, and levels of participation.

4. **Post-Test Assessment (Day 6):**
   - All participants will complete a post-test assessment identical to the pre-test to measure their knowledge and skills in cybersecurity after the intervention period.
   - The post-test scores will be compared with the pre-test scores to determine any changes or improvements.
5. **Survey (Day 6):**
   - Participants will be asked to complete a survey assessing their engagement, motivation, and perceptions of the effectiveness of the instructional methods used in the study.
   - The survey will include Likert-scale questions and open-ended prompts to gather qualitative feedback.
6. **Data Analysis:**
   - Pre-test and post-test scores will be compared between the experimental and control groups using appropriate statistical analyses (e.g., paired t-tests) to determine if there are significant differences in learning outcomes.
   - Survey responses will be analyzed descriptively to identify trends and patterns in participants' perceptions and experiences with the instructional methods.

Expected Outcomes:

- If participants in the experimental group demonstrate significantly greater improvement in cybersecurity knowledge and skills compared to the control group, it would provide preliminary support for the hypothesis that game-based learning is effective in cybersecurity education.
- Additionally, if participants in the experimental group report higher levels of engagement and motivation compared to the control group, it would further indicate the potential benefits of game-based learning approaches.

Ethical Considerations:

- Informed Consent: Participants and their parents/guardians will provide informed consent before participating in the study, detailing the purpose, procedures, and potential risks and benefits of involvement.
- Confidentiality: Participant data will be anonymized and kept confidential to protect their privacy and confidentiality.
- Debriefing: Participants will be provided with a debriefing session at the end of the study to address any questions or concerns and to inform them of the study's results.
- Ethical Approval: The study protocol will be reviewed and approved by the relevant institutional review board to ensure compliance with ethical guidelines and standards.

This pilot study aims to provide preliminary insights into the effectiveness of game-based learning in cybersecurity education, laying the groundwork for future research and larger-scale studies in this area.

5.2 Result and Analysis

Used social networks, I gathered participates from different universities who are studying cybersecurity and people are self-studying. And there were 10 participants.

5.2.1 Results

Before starting the experiment, I evaluate the knowledge about cybersecurity, and made assessment questions for the pre-test.

Assessment Questions:

1. What is the definition of cybersecurity?
2. Name three common types of cyber threats.
3. Explain the concept of phishing and provide an example.
4. Describe the importance of using strong, unique passwords for online accounts.
5. What are the potential risks of using public Wi-Fi networks?
6. Define malware and provide two examples of malware types.
7. Explain the difference between encryption and hashing.
8. Describe two-factor authentication and its role in enhancing online security.
9. What steps can individuals take to protect their personal information when using social media platforms?
10. Identify three cybersecurity best practices for safeguarding personal devices (e.g., computers, smartphones) from cyber threats.

These questions cover a range of cybersecurity topics, including terminology, common threats, security practices, and protective measures. They are designed to assess participants' baseline knowledge and skills in cybersecurity at the beginning of the study and to measure any improvements after the intervention period. Also these questions used for the post-test.

Results of the pre-test (Table 5.1, 5.2) showed that participants have a different level knowledge in cybersecurity. This helped to analyze results after the experiment (Figure 5.1, 5.2). In the experimental group, participants had more progress than the control group. And the highest progress has been by Serik from experimental group. But the highest score has been by Islam from control group. Berik and Ansar from control group had the worst score and hadn't any progress (more details of post-test showed in Table 5.3, 5.4).

In the end of experiment, participant assessed about engagement and motivation (Table 5.5, 5.6, 5.7, 5.8). These showed that the experimental group had the more motivation that control group in the period of experiments.

5.2.2 The basic analysis of results

To analyze these results, we can start by comparing the pre-test and post-test scores within each group (experimental and control) to assess any changes. Then, we can compare the changes between the experimental and control groups to determine if there are any differences attributable to the intervention. Let's break it down step by step:

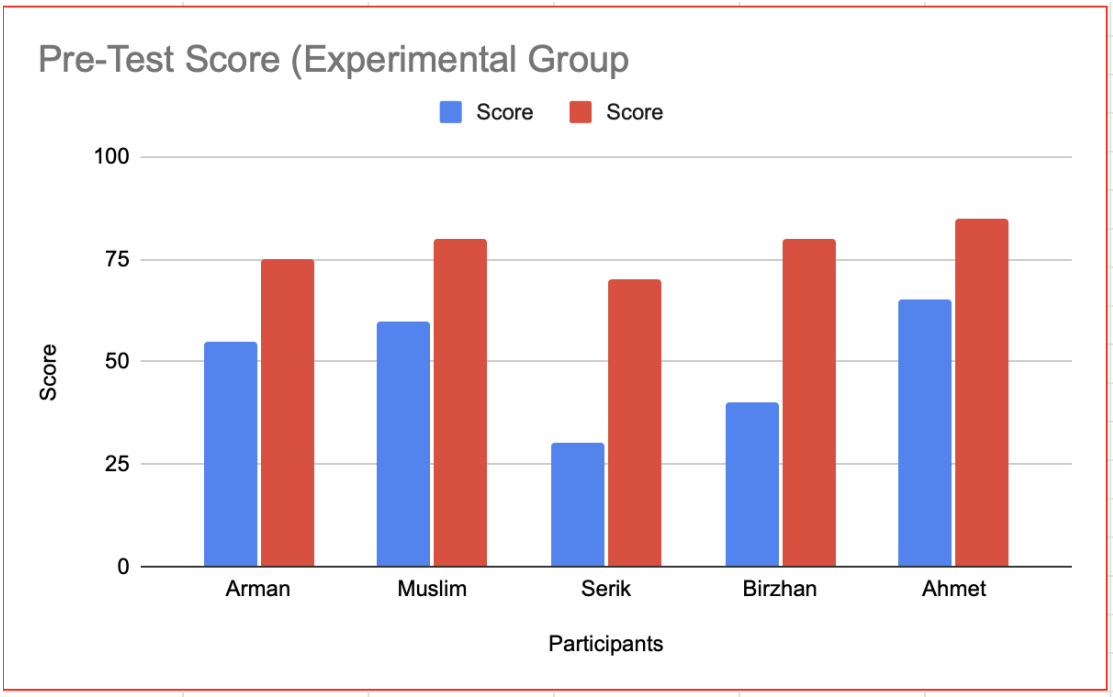

Figure 5.1 – Experemental Group

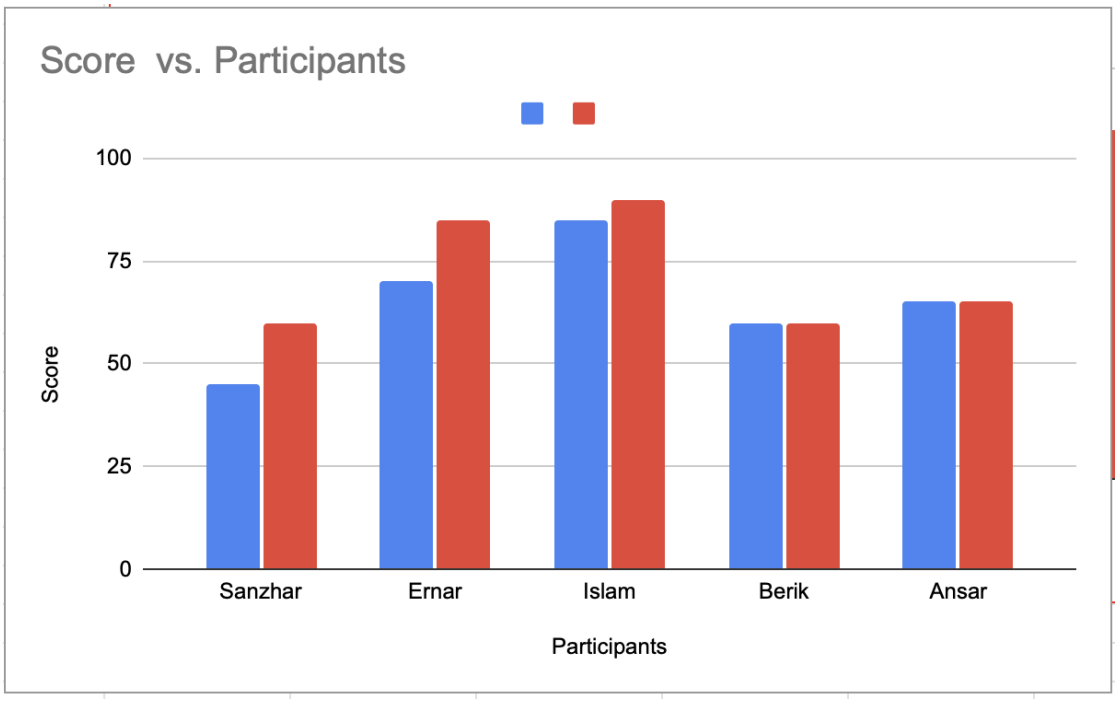

Figure 5.2 – Control Group

Calculate the Pre-Test and Post-Test Mean Scores for Each Group:
Experimental Group:
- Pre-Test Mean: (55 + 60 + 30 + 40 + 65) / 5 = 50
- Post-Test Mean: (75 + 80 + 70 + 80 + 85) / 5 = 78

Control Group:
- Pre-Test Mean: (45 + 70 + 85 + 60 + 65) / 5 = 65
- Post-Test Mean: (60 + 85 + 90 + 60 + 65) / 5 = 72

Calculate the Change in Scores for Each Participant:
Experimental Group:
- Arman: Post-Test Score (75) - Pre-Test Score (55) = 20
- Muslim: Post-Test Score (80) - Pre-Test Score (60) = 20
- Serik: Post-Test Score (70) - Pre-Test Score (30) = 40
- Birzhan: Post-Test Score (80) - Pre-Test Score (40) = 40
- Ahmet: Post-Test Score (85) - Pre-Test Score (65) = 20

Control Group:
- Sanzhar: Post-Test Score (60) - Pre-Test Score (45) = 15
- Ernar: Post-Test Score (85) - Pre-Test Score (70) = 15
- Islam: Post-Test Score (90) - Pre-Test Score (85) = 5
- Berik: Post-Test Score (60) - Pre-Test Score (60) = 0
- Ansar: Post-Test Score (65) - Pre-Test Score (65) = 0

Calculate the Mean Change in Scores for Each Group:
- Experimental Group:** (20 + 20 + 40 + 40 + 20) / 5 = 28
- Control Group:** (15 + 15 + 5 + 0 + 0) / 5 = 7

Compare the Mean Changes Between the Experimental and Control Groups:
- Experimental Group Mean Change: 28
- Control Group Mean Change: 7

The experimental group showed a higher mean change in scores compared to the control group, suggesting that the intervention had a more significant effect on improving test scores. But these was the basic analysis. To know if this difference is statistically significant, I need to do further statistical analysis like t-tests.

5.2.3 t-tests analysis of Post-Test result:

Experimental Group Post-Test Scores: 75, 80, 70, 80, 85
Control Group Post-Test Scores: 60, 85, 90, 60, 65

First, let's calculate the sample statistics:

For the Experimental Group: - Sample Mean ($\bar{x}_1$): $\frac{75+80+70+80+85}{5} = 78$ - Sample Standard Deviation (s_1): We'll use the formula for sample standard deviation:

$$s_1 = \sqrt{\frac{\sum (x - \bar{x})^2}{n - 1}} \tag{5.2.1}$$

where x represents each score in the sample, $\bar{x}$ is the sample mean, and n is the

sample size. Calculating this gives us:

$$s_1 = \sqrt{\frac{(75-78)^2 + (80-78)^2 + (70-78)^2 + (80-78)^2 + (85-78)^2}{5-1}} \approx 5.82$$

For the Control Group: - Sample Mean ($\bar{x}_2$): $\frac{60+85+90+60+65}{5} = 72$ - Sample Standard Deviation (s_2): Using the same formula, we get:

$$s_2 = \sqrt{\frac{(60-72)^2 + (85-72)^2 + (90-72)^2 + (60-72)^2 + (65-72)^2}{5-1}} \approx 12.65$$

Next, we'll calculate the t-statistic using formula (4.4.1). Substituting the values, we get:

$$t = \frac{78-72}{\sqrt{\frac{5.82^2}{5} + \frac{12.65^2}{5}}} \approx \frac{6}{\sqrt{6.695 + 40.026}} \approx \frac{6}{7.63} \approx 0.79$$

The degrees of freedom (df) for an independent samples t-test is $df = n_1 + n_2 - 2 = 5 + 5 - 2 = 8$.

Now, we'll use a t-distribution table or statistical software to find the critical value for a two-tailed test with a significance level (α) of 0.05 and $df = 8$. From the t-distribution table, $t_{\text{critical}} \approx \pm 2.306$.

Since $|t| < t_{\text{critical}}$, we fail to reject the null hypothesis.

Lastly, we would calculate the p-value associated with the t-statistic to confirm our findings. If the p-value is greater than 0.05, it would further support our decision not to reject the null hypothesis.

The p-value is 0.226153, which is greater than the significance level of 0.05, we fail to reject the null hypothesis.

This means that there is not enough evidence to conclude that there is a significant difference between the mean post-test scores of the experimental and control groups. In other words, we cannot conclude that there is a significant difference between the mean post-test scores of the experimental and control groups.

So, based on the statistical analysis, we don't have sufficient evidence to say that the intervention (experimental group) led to significantly different post-test scores compared to the control group.

Table 5.1 – Tests Score (Experimental Group)

Participants	Pre-Test Score	Post-Test Score
Arman	55	75
Muslim	60	80
Serik	30	70
Birzhan	40	80
Ahmet	65	85

Table 5.2 – Tests Score (Control Group)

Participants	Pre-Test Score	Post-Test Score
Sanzhar	45	60
Ernar	70	85
Islam	85	90
Berik	60	60
Ansar	65	65

Table 5.3 – Engagement and Motivation (Experimental Group)

Participants	Engagement	Motivation
Arman	4	4
Muslim	5	5
Serik	5	4
Birzhan	5	5
Ahmet	4	5

Table 5.4 – Engagement and Motivation (Control Group)

Participants	Engagement	Motivation
Sanzhar	3	3
Ernar	5	5
Islam	4	5
Berik	2	2
Ansar	2	2

Chapter 6

Conclusions and future work

6.1 Conclusions

The purpose of this study was to find out how the game can affect cybersecurity education. And for this, 2 groups were formed, one with the game, and the other without.

Descriptive statistics were calculated for both the experimental and control groups to provide an overview of the post-test scores. The mean post-test score for the experimental group was 78, with a standard deviation of 5.82, while the mean post-test score for the control group was 72, with a standard deviation of 12.65. This indicates that, on average, participants in the experimental group performed slightly better on the post-test compared to those in the control group. However, there was greater variability in scores within the control group.

To determine whether there was a significant difference in post-test scores between the experimental and control groups, an independent samples t-test was conducted. The null hypothesis stated that there would be no significant difference in post-test scores between the two groups.

The results of the t-test revealed a t-statistic of 0.79 with 8 degrees of freedom. The associated p-value was calculated to be 0.226153.

The p-value obtained from the t-test was greater than the predetermined significance level of 0.05. Therefore, we fail to reject the null hypothesis, indicating that there is not enough evidence to conclude that there is a significant difference in post-test scores between the experimental and control groups.

Despite expectations that the intervention would lead to improvements in post-test scores, the results did not support this hypothesis. One possible explanation for this finding could be the variability in participant response to the intervention. It is possible that some participants in the experimental group may have benefited from the intervention, while others may not have experienced any improvement in test performance.

Additionally, methodological limitations such as sample size, randomization procedures, and potential confounding variables may have influenced the outcomes of the study. For example, the sample size of the study may not have been large enough to detect small but significant differences in post-test scores between the experimental and control groups.

Furthermore, external factors such as individual motivation, prior knowledge, and environmental factors could have influenced participants' test performance, but were not controlled for in the study design.

6.2 Future work

Further research may be warranted to explore alternative interventions or to investigate potential moderators that could influence the effectiveness of the intervention. Additionally, considerations for sample size and study design should be taken into account in future investigations to ensure robust and generalizable findings.

Bibliography

[1] C. Catalin, "Google says it mitigated a 2.54 tbps ddos attack in 2017 largest known to date," *Contributor*, 2020.

[2] "Colonial pipeline boss confirms 4.4m dollar ransom payment," *BBC News*, 2021.

[3] "Musk and gates 'hacked' in apparent bitcoin scam," *BBC News*, 2020.

[4] "Cybercrime to cost the world 10.5 trillion dollar annually," *Cybercrime Magazine*, 2023.

[5] L. B. Baker and J. Finkle, "Sony playstation suffers massive data breach," *Reuters*, vol. 26, p. 43, 4 April 2011.

[6] J. Markoff, "A robot network seeks to enlist your computer," *New York Times*, vol. 21, 11 October 2008.

[7] M. Prensky, "Fun, play and games: What makes games engaging," *Digital Game-Based Learning*, vol. 5, no. 1, pp. 5–31, 2001.

[8] A. J. M. a. S. A. Nagarajan, Ajay, "Exploring game design for cybersecurity training," *IEEE International Conference on Cyber Technology in Automation*, pp. 256–262, 05 May 2012.

[9] M. K. a. I. Mavridis, "Evaluation of hacklearn cofelet game user experience for cybersecurity education," *International Journal of Serious Games*, vol. 8, no. 3, pp. 3–24, 2021.

[10] T.-H. K. J. H. G. Jin, M. Tu and J. White, "Evaluation of game-based learning in cybersecurity education for high school students," *Journal of Education and Learning*, vol. 12, no. 1, pp. 150–158, 2018.

[11] M. O. et al., "Securityempire: Development and evaluation of a digital game to promote cybersecurity education," 2014.

[12] M. F. T. B. D. Cone, C. E. Irvine and T. D. Nguyen, "A video game for cyber security training and awareness," *computers security*, vol. 26, no. 1, pp. 63–72, 2007.