UNIVERSITY OF SOUTHAMPTON
Faculty of Engineering and Physical Sciences
School of Electronics and Computer Science

A project progress report submitted for the award of
BSc Computer Science

Supervisor: Dr Nawfal Fadhel
Examiner: Dr Indu Bodala

Enhancing Adults' Understanding of Security Concepts through a Cybersecurity Game

by William Mayhew

April 29, 2024

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF ENGINEERING AND PHYSICAL SCIENCES
SCHOOL OF ELECTRONICS AND COMPUTER SCIENCE

A project report submitted for the award of BSc Computer Science

by William Mayhew

The increasing complexity of cyber threats necessitates enhanced understanding and awareness of mitigation strategies. To confront this challenge, an educational escape room game was developed. Previous studies have shown that educational games can lead to academic improvements, thus an attempt to teach those who are susceptible to cyber risks about security concepts and mitigation strategies was made. The report reviews various cyberattacks, human vulnerabilities and associated crimes to underpin the game's core purpose. Various gamification techniques have been discussed to assist in the development strategy to ensure that an educational, engaging, and fun game was developed. The end product was tested on various participants in order to determine its effectiveness in enhancing understanding and awareness of cyber threats.

Statement of Originality

- I have read and understood the ECS Academic Integrity information and the University's Academic Integrity Guidance for Students.
- I am aware that failure to act in accordance with the Regulations Governing Academic Integrity may lead to the imposition of penalties which, for the most serious cases, may include termination of programme.
- I consent to the University copying and distributing any or all of my work in any form and using third parties (who may be based outside the EU/EEA) to verify whether my work contains plagiarised material, and for quality assurance purposes.

I have acknowledged all sources, and identified any content taken from elsewhere.

I have used various resources produced by someone else, which can be found at the following links:

2D Pixel Art Icons - Swords
2D Pixel Item Asset Pack
Pixel Art Key Pack - Animated
Rogue Fantasy Castle
Tiny RPG - Forest
Pixel Art Top Down - Basic
Ink Integration for Unity
Ultimate A* Pathfinding Solution
Fantasy RPG Chests
Necromancer
Effect and Bullet
zxcvbn-cs by Dropbox

I did all the work myself, or with my allocated group, and have not helped anyone else.

The material in the report is genuine, and I have included all my data/code/designs.

I have not submitted any part of this work for another assessment.

My work involved human participants in an anonymous survey. The ethics approval reference number is ERGO/FEPS/92262

Acknowledgements

I would like to express my deepest gratitude to Dr. Nawfal Fadhel, whose unwavering support has been instrumental throughout every phase of this project.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This paper will explore the different cyber attacks and crimes prominent in the modern-day, as well as the use of gamification techniques to combat these challenges.

1.1 Research Problem

From 2017 to 2022, a survey conducted by the UK Government found that the proportion of UK businesses identifying cyber attacks each year fluctuated between 32% and 46% [1]. The findings also suggested that less cyber mature organisations were likely underreporting meaning these percentages were likely higher.

Phishing attempts emerged as the predominant cyber attack affecting businesses, constituting a staggering 83% of the total identified attacks. This suggests that the main vulnerability behind these malicious attacks is humans. Studies have also shown that humans are a major vulnerability where most successful attacks were attributed to human error [1].

In 2022, 54% of businesses took proactive measures to detect and address cybersecurity risks. However, only 19% of businesses utilised staff testing despite phishing being the predominant cyber attack[1]. This discrepancy highlights a notable gap in addressing human vulnerabilities through adequate training and education in cybersecurity.

[1] *Cyber Security Breaches Survey 2022* by GOV.UK. Available at https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022. Accessed on November 11, 2023.

1.2 Research Question

The primary focus of this research is to explore and identify an optimal technological approach to mitigating cybersecurity threats. An approach utilising gamification techniques will be utilised to enhance cybersecurity awareness as this has been shown to promote engagement and participation to improve academic performance [2].

Research Question

How effective is a cybersecurity game at teaching cybersecurity concepts?

1.3 Scope

Focusing on the prevalent challenges presented by phishing attacks, this study investigates the use of gamification strategies in cybersecurity education tailored for adults. The research aims to develop an application through Unity, serving as an educational tool across both professional and personal settings. However, it is essential to note that the project's scope will primarily address fundamental mitigation techniques concerning phishing and other common human vulnerability attacks like scareware. While aiming to enhance awareness, this project will not delve into more intricate or technical aspects of cybersecurity threats.

Chapter 2

Literature Review

This chapter conducts a review of the current state of cyber-attacks, exploring their scale and various associated crimes.

2.1 Cyber-Attacks

Cyber-attacks cover a broad spectrum of malicious activities orchestrated by individuals or groups aiming to compromise systems or networks. The following sections provide insight into the different types of attacks, their scale, and the vulnerabilities contributing to these attacks.

2.1.1 Social Engineering

Social engineering is a sophisticated technique employed in cyber attacks exploiting human psychology to obtain sensitive information or prompt actions. Alsharif et al's study highlights humans as a major vulnerability, attributing over 39% of security risks and 95% of successful attacks to human error [1].

Common social engineering techniques include Phishing, Scareware, and Spear Phishing [1], [3], [4], enabling fraudulent activities and scams, including romance and friendship scams.

2.1.2 Phishing

Phishing, a common cyber attack, deceives users into performing ’wrong’ actions to reveal sensitive data like passwords or financial details. In a UK Government Survey (2022), 39% of businesses experienced cyber attacks, with phishing as the top threat at 83% [1]. Phishing primarily occurs via voice, SMS, and the Internet [3]–[5]. Across phishing studies, emails consistently emerge as a recurring vector due to their widespread use and simplicity in sending emails to many individuals simultaneously [4], [6].

Deceptive phishing, the most common type, involves attacks using social engineering to mislead victims by impersonating trusted entities. Attackers impersonate recognised entities to trick the user into believing a fabricated scenario and clicking on malicious links to steal sensitive information [4]. An example of this includes email spoofing to mimic legitimate sources. This is achieved by copying the aesthetics of a trusted email and/or sending it from an email address that looks very similar to that of a trusted email. These emails will typically have an embedded link redirecting the user to a fake website [6].

2.1.3 Scareware

Scareware manipulates victims through false alarms and fake threats, prompting them to believe their systems are infected. Attackers then offer a ’solution’, leading victims to give information or grant access to the attacker. Intrusive pop-ups will have messages like ”Your device is infected” [3].

Ransomware is malware that encrypts users’ documents, then asks for a fee to decrypt them [7]. In a review conducted by McIntosh et al, the link between scareware and ransomware was defined differently. One study stated that ransomware is a class of scareware where scareware can lead to the implementation of ransomware [8]. Another stated that scareware is not considered a type of ransomware as it falsely informs the users that they are infected [8]. Most researchers considered that scareware is not a type of ransomware, but due to the link between them, we will consider them both, where ransomware is the risk of being targeted by scareware [8].

2.1.4 Spear Phishing

Spear Phishing, a sophisticated form of regular phishing, targets specific individuals or organisations, employing various communication channels like emails, instant messaging, and social media. The success rate surpasses regular phishing as the emails mimic trusted sources such as a friend or colleague, leading victims to trust and engage with them [5].

2.2 Crimes

After exploring cyber attacks such as social engineering, phishing, scareware, and spear phishing, this section delves into the subsequent crimes enabled by these attacks. They serve as initial assaults, exploiting victims and notably enabling fraudulent activities.

2.2.1 Fraud

Fraudulent activities pose a significant threat to individuals and businesses. According to a UK Government policy paper in 2022[2], fraud accounted for over 40% of all crimes, with an estimated 3.7 million incidents in England and Wales. The Guardian[3] reported scammers stole over £1.2 billion from UK consumers in 2022, affecting individuals with losses ranging from £100 to six figures, including cases involving life savings. Notably, an economic crime survey[4] found that vectors used against businesses included email (24%), hacking (22%), in-person (19%), and phone-based (19%).

An illustrative case published by The Guardian[3] involved fraudsters posing as solicitors who instructed a couple to transfer their housing deposit into a compromised account using email addresses closely resembling that of a genuine law firm's.

[2] Fraud Strategy: Stopping scams and protecting the public (accessible), GOV.UK. Available at https://www.gov.uk/government/publications/fraud-strategy/fraud-strategy-stopping-scams-and-protecting-the-public (visited on 11/11/2023).

[3] 'I Lost £240,000': UK Fraud Victims Share Their Stories, by Anna Tims and Rupert Jones, The Guardian. Available at https://www.theguardian.com/money/2023/oct/07/i-lost-240000-uk-victims-share-their-stories (visited on 11/11/2023)

[4] Economic Crime Survey 2020 (accessible), by GOV.UK. Available at https://www.gov.uk/government/publications/economic-crime-survey-2020/economic-crime-survey-2020 (visited on 11/11/2023)

2.2.2 Romance and Friendship Scams

Romance and friendship scams exploit individuals seeking connections, tricking them into sending money for financial gain. Lloyds Bank[5] reported victims losing an average of £8,000, with the most vulnerable group aged between 65 and 74.

Regardless of age, these scams can target anyone vulnerable. For instance, a case involved 'Zainab' (pseudonym) encountering a scammer on a dating site who faked a cancer diagnosis and COVID contraction. The scammers successfully persuaded Zainab to send £6,150 for supposed bills[6].

2.3 Policies

To minimise vulnerabilities in users and reduce the potential for attacks, strong and relevant cyber policies are necessary. This section reviews practices which are being implemented by organisations and the common shortcomings.

2.3.1 Password Policies

Effective password security policies play a critical role in safeguarding user accounts and sensitive information. Despite this, a review conducted by Kevin Lee et al. found that only 13% of websites followed all relevant password policy practices [9]. Key practices which were discussed include blocklists against common words/passwords, strength meters and minimum strength requirements, and composition policies allowing for freedom in character sets used in passwords.

However, the review highlighted some shortcomings in current password policy implementations. For instance, most organisations rely solely on calculating password complexity rather than considering guessability [9].

[5] Criminals turn to romance scams as reports soar by 30%, by Lloyds Banking Group. Available at https://www.lloydsbankinggroup.com/media/press-releases/2023/lloyds-bank-2023/criminals-turn-to-romance-scams-as-reports-soar-by-30-per-cent.html (visited on 11/11/2023)

[6] 'I've Lost All Confidence in People': What It's like to Be Victim of £6k Romance Fraud. Grace Gausden. Available at https://inews.co.uk/inews-lifestyle/money/saving-and-banking/romance-fraud-couldnt-pay-rent-lose-confidence-people-2147294. (visited on 11/11/23)

To address this issue, the review suggested the implementation of *zxcvbn*, a password strength estimation tool developed by Dropbox [10]. Utilising dictionaries of common words and previously exposed passwords from data breaches, zxcvbn provides a more accurate estimate of how long a password may take to crack

2.3.2 Human-Centric Cybersecurity Policies

Stemming from the cyber attacks previously discussed, cyber policies help ensure stronger practices are executed by users to protect themselves and any organisations they might be linked with.

A review conducted by Maalem Lahcen et al, emphasised the importance of behavioural aspects in cybersecurity policies [11]. The study underscored the necessity for users to comprehend the risks associated with cyber threats and discern between desired and undesired behaviours. However, it also highlighted that a ”one size fits all” approach to policy formulation may not be as effective due to internal biases towards security. As a result, policies should be tailored to users based on factors such as their level of knowledge, access privileges, responsibilities, and other pertinent considerations. Such personalised policies are better posed to address the diverse needs and challenges faced by users.

2.4 Discussion

The literature review provides valuable insights into the landscape of cyber-attacks, shedding light on the techniques employed, the crimes they spawn, and the potential policies to address them. The vulnerabilities caused by social engineering highlight the crucial significance of human factors in cyber security breaches [1]. These exploitative practices pave the way for crimes such as fraud to take place, which are shown to be extremely prevalent in the modern age[2]. As well as this, the increasing sophistication of these attacks makes it harder to consistently defend against these attacks, especially for those who lack this knowledge.

Implementing relevant cyber security policies is also essential to mitigate human vulnerabilities. Users must comprehend what constitutes good and bad cybersecurity practices, underscoring the necessity for a robust policy framework [11].

In light of the increasing prevalence and complexity of cyber threats, strengthening cybersecurity safeguards is critical to ensure human vulnerabilities are minimised.

Chapter 3

Gamification

Gamification involves applying game characteristics in non-game contexts [12]. In education, it aims to enhance extrinsic and intrinsic motivation, prompting engagement and learning [2]. Extrinsic motivation involves external rewards, while intrinsic motivation is driven by interest and enjoyment [13].

Gamification strategies serve as tools in the integration of game elements in non-game contexts. Two commonly referenced approaches include MDA (Mechanics-Dynamics-Aesthetics) and Octalysis [2], [14]–[16].

The field of gamification is vast, as demonstrated in a systematic review by Mora et al which uncovered around 40 different frameworks. However, many of these frameworks are built upon the core principles of the previously mentioned models (MDA and Octalysis) and so they will be the focus of the following section [17].

3.1 MDA Framework

MDA is built from three essential components: Mechanics, Dynamics, and Aesthetics. Mechanics are the fundamental rules and components that control game interactions within an environment (e.g. Weapons in a shooter game); Dynamics are the behaviours and interactions resulting from the mechanics in action, creating experiences (e.g. Ability to earn new weapons); and Aesthetics evoke emotional responses and experiences due to the mechanics and dynamics together (e.g. Sense of accomplishment) [16]. To describe the aesthetics, Hunicke et al provides a basic list of vocabulary which the game should tend towards [16]:

- Sensation
- Fantasy
- Narrative
- Challenge
- Fellowship
- Discovery
- Expression
- Submission

MDA's simplicity allows for clear structuring and emphasises aesthetic goals. This allows us to fine-tune and increase specificity to our desired outcome [16]. However, MDA might lack deeper guidelines by being too simple and not specifying requirements enough.

3.2 Octalysis

The Octalysis framework revolves around the concept of balancing the eight core drives to optimise motivation [18]. However, three studies from [15], [19], [20] utilised a series of questions to analyse the different motivations of the participants across three different audiences (students, elderly, and customers of unknown age). It revealed that balancing these drives is much harder and could require multiple iterations to tailor it to the user's motivational needs.

All studies found that Accomplishment, Empowerment, and Social Influence were identified as predominant motivational factors, while the other core drives were inconsistent. For example, [15] and [20] identified that Meaning has great motivational influence while another [19] showed extremely low influence for Meaning. However, all studies showed that Avoidance was of the lowest influence. This shows the difficulty in optimisation using Octalysis because different audiences and age ranges will demonstrate different motivational influences, requiring significant tailoring to the specific person.

3.3 Other Frameworks

Other frameworks include 6D [21] developed by Werbach and Hunter, and another developed by Nah et al [22].

6D presents a framework comprised of 6 steps: Define business objectives, Delineate target behaviours, Describe your players, Devise activity cycles, Don't forget the fun, and Deploy the appropriate tools [21]. While 6D outlines key components to a successful end product, it does not provide us with a clear strategy on how to implement and combine these different components. 6D is also business focused, and may not be easily adapted into an educational scenario [19], [23].

The framework developed by Nah et al defines 5 key principles: Goal orientation, Achievement, Reinforcement, Competition, and Fun orientation [22]. However, the lack of educational elements could reduce its effectiveness. The overemphasis on enjoyment through rewards (achievement, reinforcement) as well as competition and fun orientation might shift the focus from learning for the sake of knowledge to learning for the sake of earning rewards.

3.4 Choosing the Ideal Gamification Framework

When selecting an appropriate gamification framework for implementation, the decision rests upon the application and the desired outcome.

MDA's simplicity and clear structuring with its formal and iterative approach make it an attractive choice. However, the simplistic nature might lack deeper guidelines, potentially limiting its effectiveness in intricate scenarios. On the other hand, Octalysis offers a comprehensive approach with eight core drives to optimise motivation. Nevertheless, its implementation complexity becomes apparent as studies reveal varying motivational influences. The challenge lies in tailoring the framework to suit diverse individual needs.

I will not be considering the 6D framework and the framework by Nah et al. due to the primary focus of them both. 6D primarily focuses on business objectives and may not seamlessly translate into an education scenario, and Nah et al.'s framework overemphasises rewards and may shift the focus away from educational motivation.

In the context of developing an educational game tailored for adults, I believe MDA would be the more appropriate choice. Its simplicity enables clear structuring of the specific goal while still keeping an emphasis on the learning experience. Opting for Octalysis might introduce excessive complexity, especially with regard to tailoring different challenges for the different skill levels. Without a clear understanding of the different motivational factors of the audience, balancing the core drives while keeping it engaging could be an issue.

3.5 Discussion

To combat the issue of the aforementioned cyber security vulnerabilities, I have chosen a gamification approach to create an educational game. Gamification uses motivational drivers of human behaviour to promote engagement and participation. Studies have shown that in education, the use of gamification led to academic performance improvements [2]. The selected gamification framework to address these cybersecurity challenges is the MDA model. This will provide a structured approach with an emphasis on user experience, aligning with the goal of creating an immersive learning environment. I had also considered the Octalysis framework but decided that due to its difficult nature in refinement, it may lead to over-complication of the design of the game.

Chapter 4

Requirements Analysis

The requirements analysis outlines the features which the game should exhibit. Personas are developed and refined into user stories to identify the requirements of the system. Using the MoSCoW (Must have, Should have, Could have, Won't have) method, the features are organised into different priorities to understand what will and will not be implemented.

4.1 Personas

To understand the requirements of the game, personas have been developed to inform us about the needs of the users with their unique characteristics and different goals.

4.1.1 Persona A - Rebecca Morrow, Age 25 - P1

Rebecca is a recent graduate who is about to begin their career in sales. She has previously completed internships in related fields so is aware of the new tasks at hand. Her primary responsibilities include responding to inquiries and pitching products and services through various communication channels like email. She will work in a dynamic sales environment, having to respond to a high volume of emails quickly.

In her internships, Rebecca had almost fallen victim to a spear-phishing attack if it was not for her supervisor who stepped in. She wants to ensure that this does not happen again. Rebecca is keen on developing her cyber security awareness to protect herself and the company from any malicious attacks she may encounter.

4.1.2 Persona B - Steve Cooper, Age 42 - P2

Steve is a middle aged professional managing a small medical practice. His primary responsibilities include administrative tasks such as responding to client emails and management of medical records. He relies on various technologies for efficient and secure operations.

Steve is aware of the potential cyber security risks associated with managing sensitive patient data and is committed to minimising vulnerabilities. He plans to initiate regular workshops for his staff, emphasising the importance of cyber security. Additionally, Steve is eager to make these workshops engaging and believes that incorporating a game-based approach would keep the sessions fun but also provide practical and engaging ways for his team to learn and apply cybersecurity concepts.

4.1.3 Persona C - Velma Summers, Age 67 - P3

Velma is a retired teacher and mother of two, leading an active post-retirement life by engaging in various community activities. She lives alone following the passing of her husband a few years ago. She values social connections, enjoys making new friends, and is always willing to lend a helping hand to those in need. Velma has recently begun using social media to keep in touch with her newfound friends and expand her social circle.

However, Velma's children have expressed concerns about her potential vulnerability to online scams due to her trusting nature. While she's tried to familiarise herself with warning signs, she's uncertain about her full grasp of them. Velma believes that practical cases or real-life examples would reinforce her understanding of cyber attacks and better equip her to identify potential scams online.

4.2 User Stories

The following user stories are derived from the different personas to describe the various features of the system.

The Story ID, structured as "[Persona ID]-[Story Number]", serves as a unique identifier linking each user story to a specific persona.

Table 4.1: User Stories

Story ID	User Story
P1-S1	As Rebecca, I want simulated scenarios involving phishing attacks through emails as well as other vectors like instant messaging, so that I can practice identifying cyber threats across different platforms.
P1-S2	As Rebecca, I want feedback on my decisions during simulated scenarios, so that I can learn from mistakes and reinforce good practices.
P1-S3	As Rebecca, I want there to be a time limit to recreate the fast-paced work environment, so that I can learn to identify threats quickly.
P2-S1	As Steve, I want a comprehensive workshop mode with customise content, so that I can tailor sessions based on specific cybersecurity challenges.
P2-S2	As Steve, I want to be able to view analytics on user performance in the different challenges, so that I can identify strengths and weaknesses to further improve and plan for future sessions.
P2-S3	As Steve, I want simulated scenarios depicting scareware tactics, so that myself and the staff are able to recognise and respond to false alarms or pop-ups attempting to compromise our systems.
P2-S4	As Steve, I want the game to feature a leaderboard, so that my staff are kept engaged, encouraging active participation through competition.
P2-S5	As Steve, I want the game to be available on different platforms, so that my staff can play the game with their own devices.
P3-S1	As Velma, I want relatable scenarios illustrating common online scams on social platforms, so that I can improve my understanding of the potential threats I might encounter.
P3-S2	As Velma, I want an easy-to-navigate interface with clear instructions, so that I can access the different games easily as I am less familiar with these technologies.
P3-S3	As Velma, I want the game to offer educational materials explaining the signs and indicators of cyber threats, so that I can understand these risks before having scenario practice.
P3-S4	As Velma, I want accessibility features such as adjustable font sizes and themes, so that I can customise it to suit my needs.

Table 4.2: Functional Requirements

ID	Requirement	MoSCoW	User Story Ref
1	Users can create an account	Could	
2	Users can login to their account	Could	
3	Users can manage their account	Could	
4	Users can navigate a user interface	Must	P3-S1
5	Users can access learning material for various cybersecurity topics	Should	P3-S2
6	Users can play scenario simulations of attacks	Must	P1-S1, P2-S3, P2-S5
7	The game will provide an introduction with instructions for each challenge	Must	P3-S1
8	The challenges will have time-limits	Must	P1-S3
9	Users can view performance analytics	Should	P1-S2, P2-S2
10	The game will provide the user with their strengths and weaknesses	Could	P1-S2, P2-S2
11	Users can view a performance leaderboard	Could	P2-S4
12	Users can customise the game visually by increasing font size and changing themes	Should	P3-S3
13	Users can play against others (multiplayer)	Won't	P2-S4
14	Users are rewarded dependent on how well they perform (time, failures)	Must	P1-S3
15	Users can customise what content is shown	Could	P2-S1
16	Users can receive hints/clues if they are stuck	Could	P1-S2
17	The game will provide an initial tutorial to understand the games mechanics	Must	P3-S2
18	Users are punished for failures	Must	
19	The game will be level based to accommodate for further expansion	Must	

4.3 Functional Requirements

The functional requirements outline the specific features and functionalities which are deemed necessary by the end user.

Table 4.3: Non-Functional Requirements

ID	Requirement	MoSCoW	User Story Ref
1	The game will be responsive	Must	
2	The game will not stutter	Must	
3	The interface should be intuitive	Must	P3-S1
4	The interface should be user-friendly	Must	P3-S1
5	The game will provide clear instructions to the user	Must	P3-S1
6	The game will provide guidance to the user	Must	P3-S1
7	The game will be compatible with different devices	Could	P2-S5
8	The game will be compatible on different operating systems	Could	
9	The game will store users details securely	Must	
10	The game will be consistent with accessibility customisations	Should	P3-S1
11	The user will strengthen their cybersecurity knowledge	Must	P1-S1, P1-S2, P2-S3, P2-S5, P3-S3
12	The game will be relatable to real-life scenarios	Must	P1-S1, P2-S3, P2-S5

4.4 Non-Functional Requirements

The non-functional requirements outline the quality constraints that the system must satisfy.

Chapter 5

The Proposed Final Design

The proposed final design of the application is an escape room concept, challenging players with cybersecurity tasks to gather resources and ultimately escape to win. Utilising the MDA framework, the game aims to encompass key motivational factors - accomplishment, empowerment, and social influence - uncovered in the review of the Octalysis framework.

Extending from the core requirements in Chapter 3, these foundational elements will guide and shape the development of the game design.

5.1 UI Wireframe

For the design of the game, a 2D top-down approach has been opted for due to its simplicity in development and visuals. The development of a 2D game is generally less complex than 3D games, requiring fewer resources in terms of assets, programming, and computational power. A top-down perspective will also offer a clear view of the room, facilitating easier navigation and understanding of the environment for players.

The UI Wireframes will serve as a design blueprint, outlining the structure and layout of the game.

5.1.1 Example Room

Figure 5.1 depicts an example room's wireframe for players, featuring interactive elements triggering challenges or messages. Non-interactive elements serve aesthetic purposes. The door serves as an exit to another room or to advance levels. Interactive elements present cybersecurity challenges, granting resources upon completion. Players can view their current inventory and elapsed time.

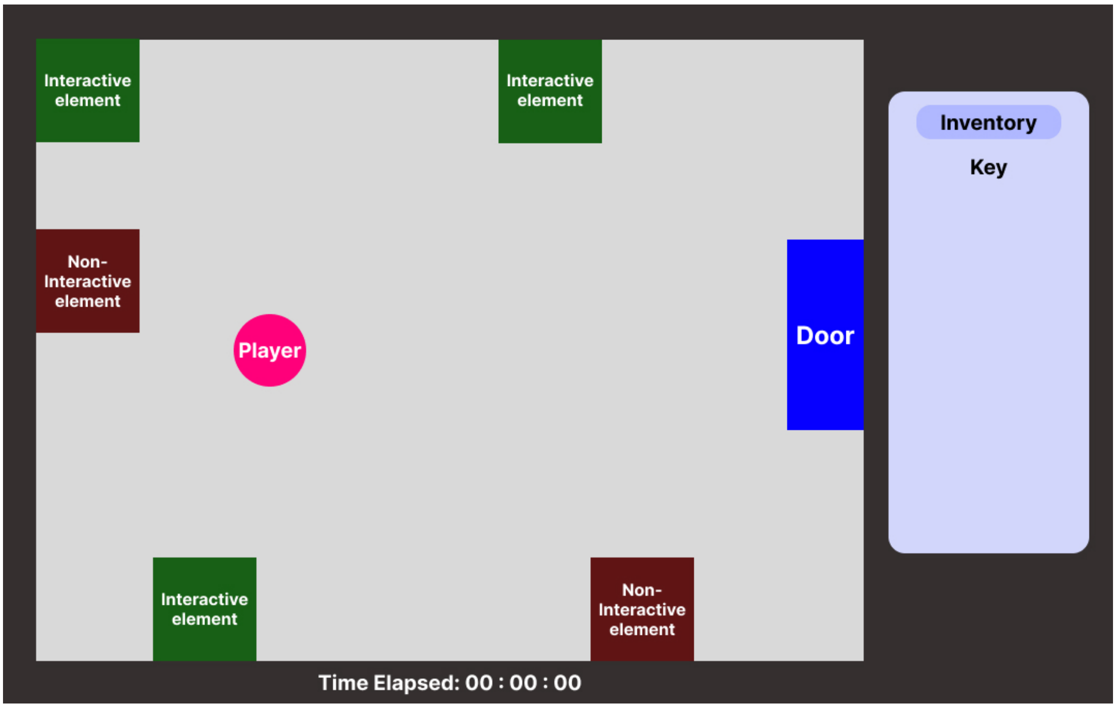


FIGURE 5.1: Wireframe: Game Level

5.1.2 Example Challenges

Figure 5.2 depicts a phishing email detection challenge. It mimics an abstract version of an email reader, where the player has to correctly identify which emails are legitimate and which are malicious.

Figure 5.3 depicts a romance and friendship scam dialogue challenge. It mimics a conversation with the player and a fraudulent user. The player must correctly choose the appropriate response options to pass.

Figure 5.4 depicts a password workshop. The player will be required to enter a password complying with the displayed rules.

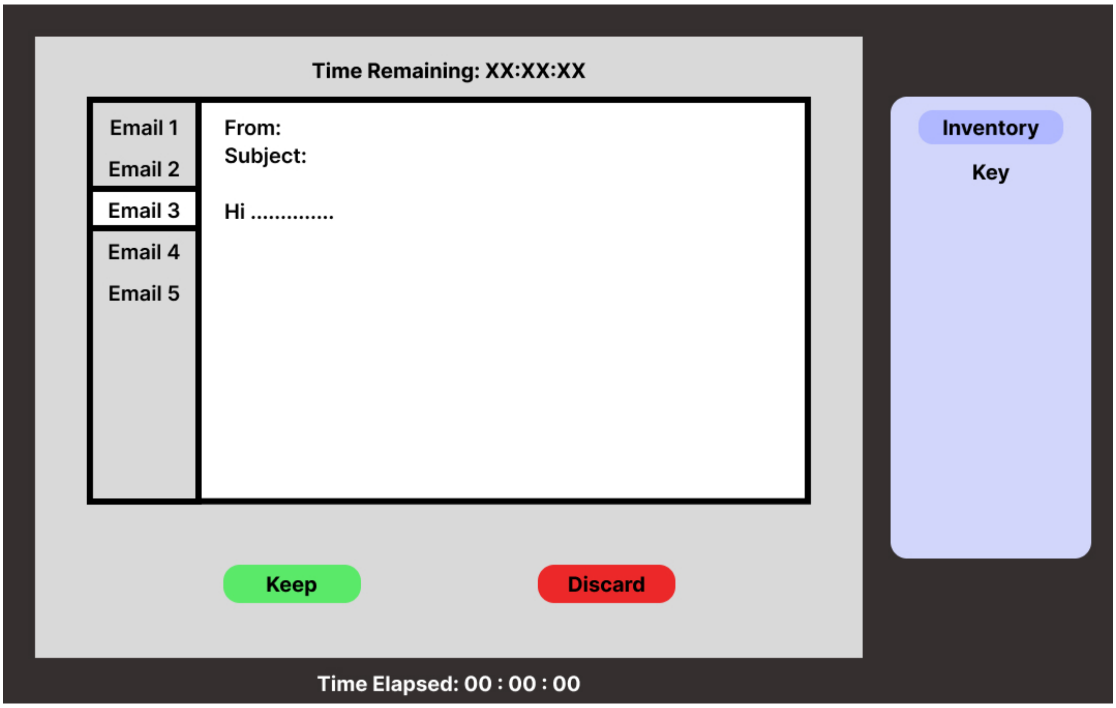


Figure 5.2: Wireframe: Phishing Email Challenge

Figure 5.5 depicts a strong password identifier challenge. The player will be required to identify which of the displayed passwords is the strongest.

Figure 5.6 depicts a bad policy identifier challenge. The player will be required to identify which of the displayed policies is the worst.

Figure 5.7 depicts a scareware pop-up challenge. Mimicking pop-ups, throughout gameplay a scareware pop-up will appear requiring the player to navigate it correctly.

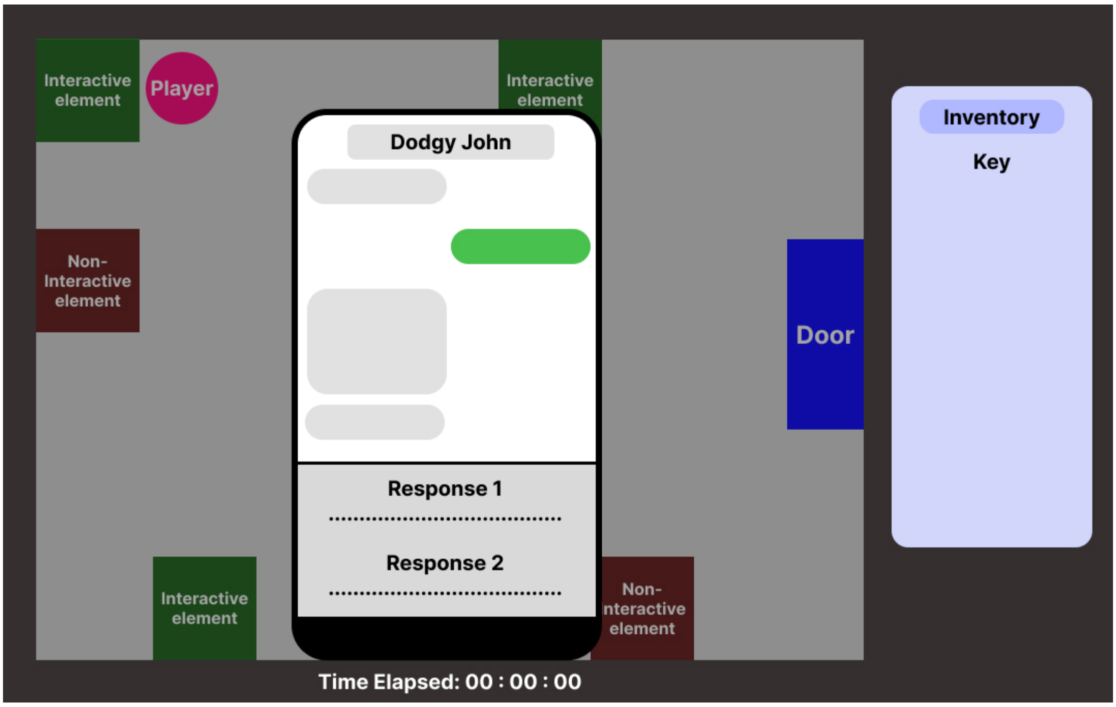


FIGURE 5.3: Wireframe: Romance and Friendship Scam Challenge

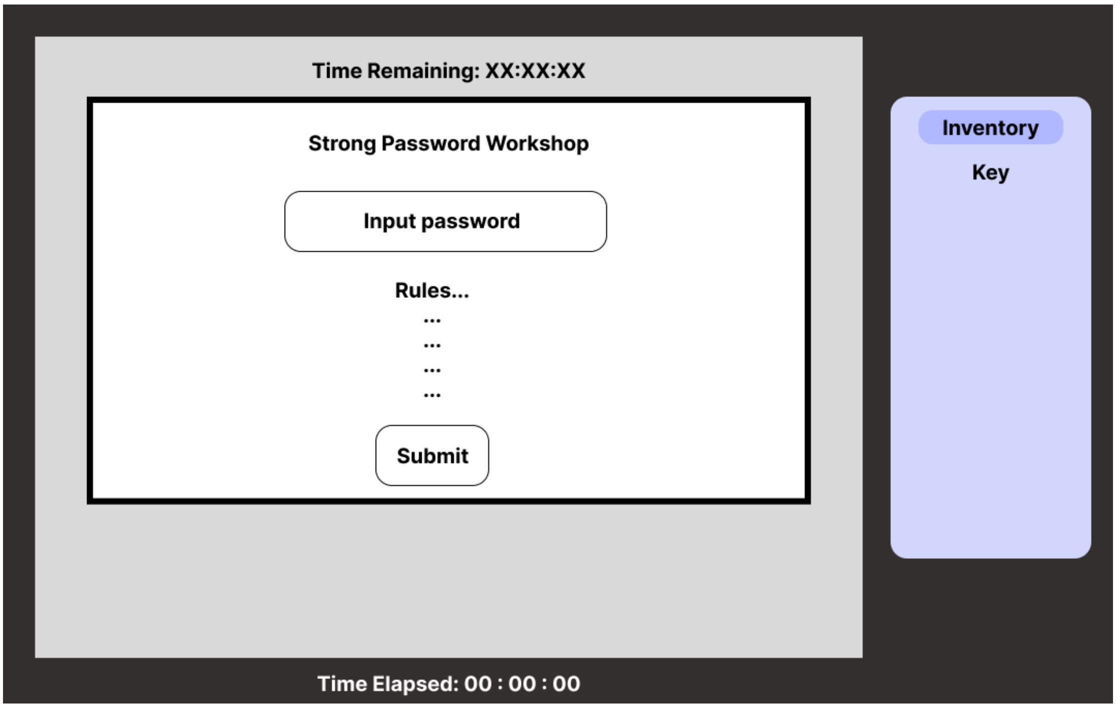
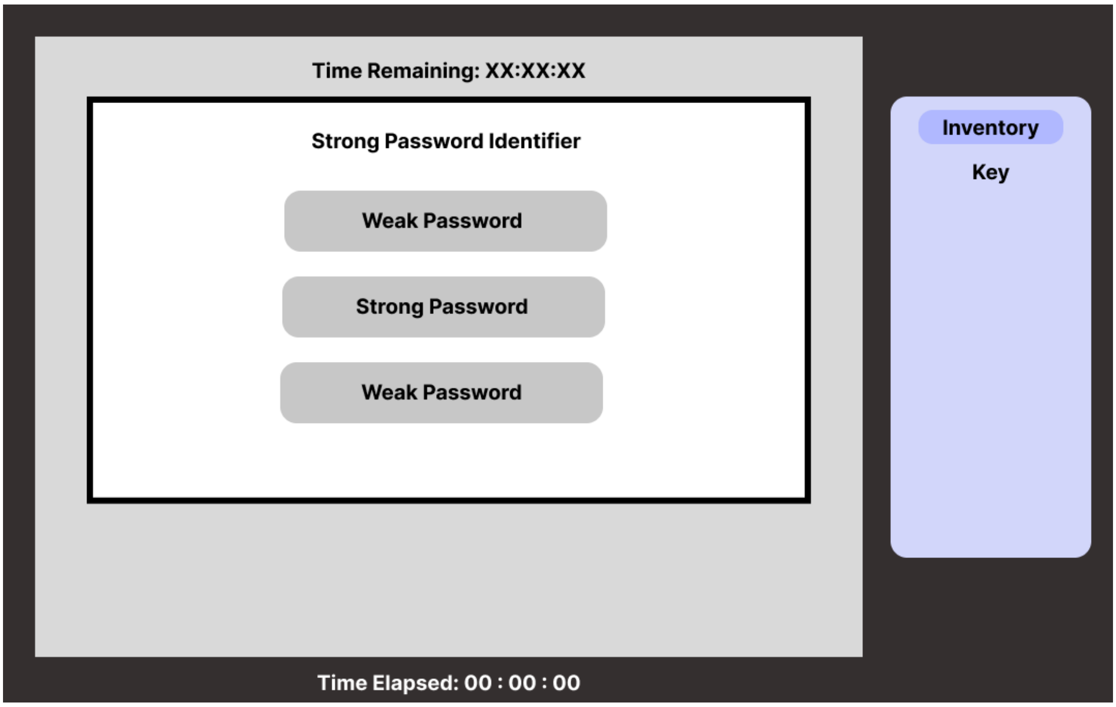


FIGURE 5.4: Wireframe: Password Workshop Challenge

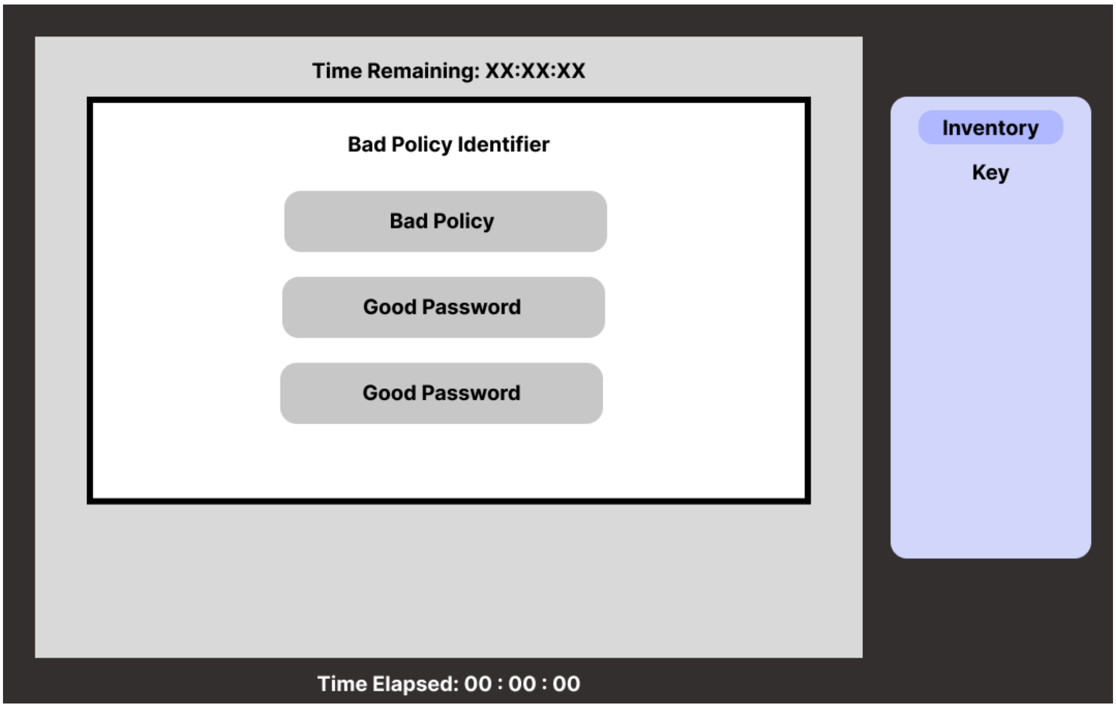


Time Remaining: XX:XX:XX

Strong Password Identifier

Time Elapsed: 00 : 00 : 00

Figure 5.5: Wireframe: Strong Password Identifier Challenge



Time Remaining: XX:XX:XX

Bad Policy Identifier

Time Elapsed: 00 : 00 : 00

Figure 5.6: Wireframe: Bad Policy Identifier Challenge

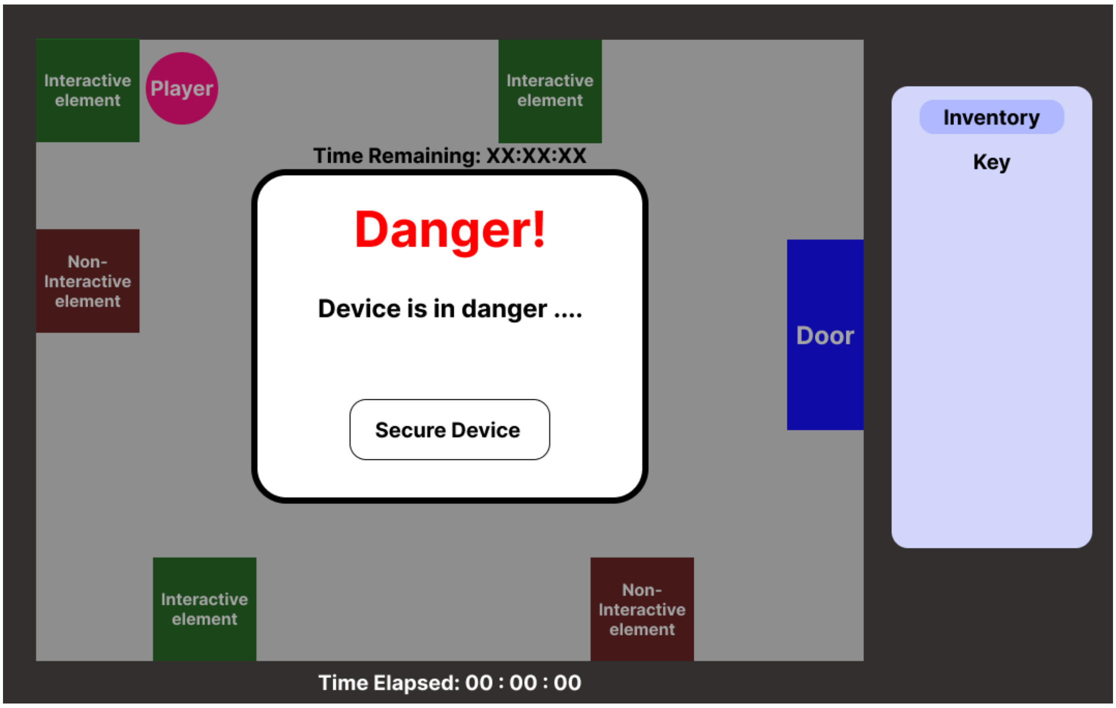


FIGURE 5.7: Wireframe: Scareware Pop-up Challenge

5.2 Activity Diagram

In Figure 5.8, the activity diagram illustrates the gameplay, omitting specific challenge steps. Initially, the player begins in a room and can interact with various objects (referenced in Figure 5.1). If encountering a door, the player can enter a new room or escape given they have a key. Interacting with objects requires the relevant resource for challenge access and failure prompts further search. Successful challenge completion yields a resource and failure results in life loss. Running out of lives ends the game, while escaping with the key leads to victory.

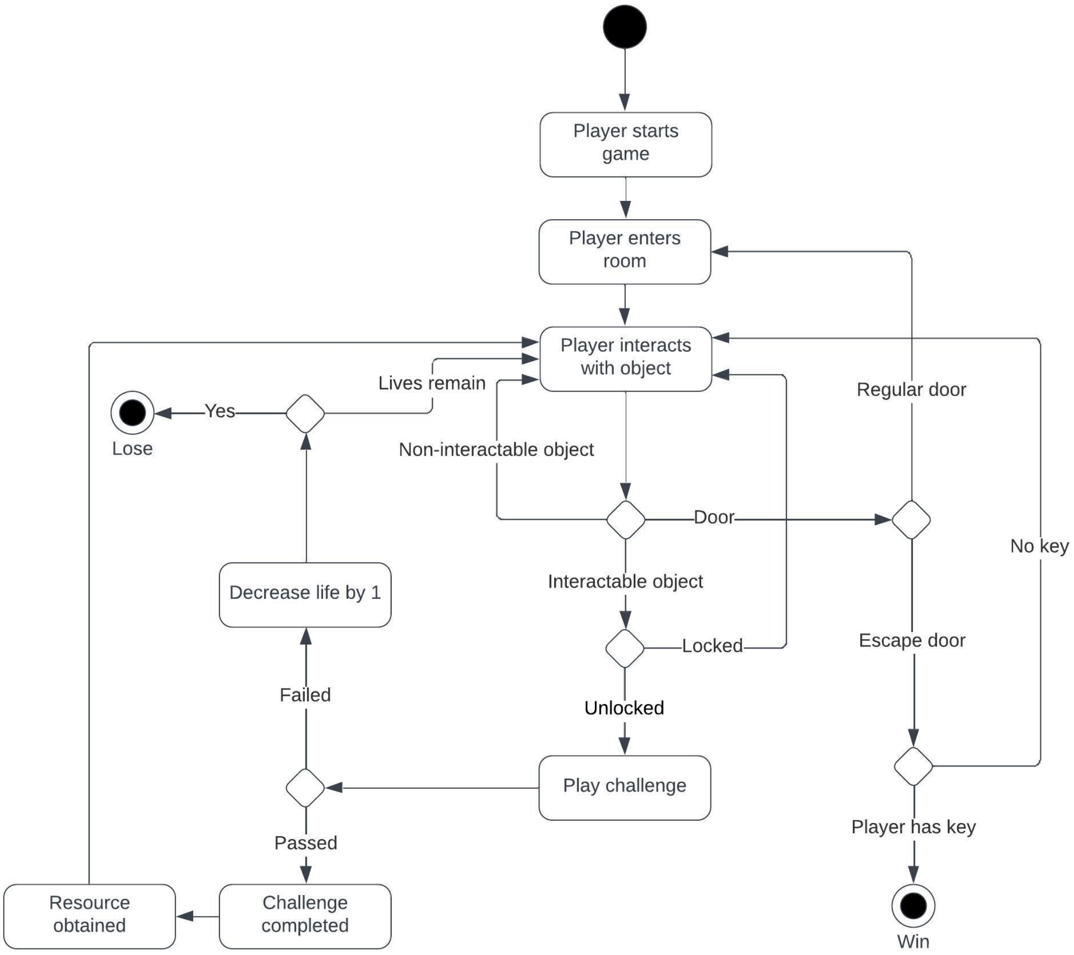


FIGURE 5.8: Activity Diagram: Escape Room

5.2.1 Challenges

Figure 5.9 shows an activity diagram illustrating the steps each challenge will take albeit each challenge will vary slightly. This can occur at the "Play challenge" state in Figure 5.8.

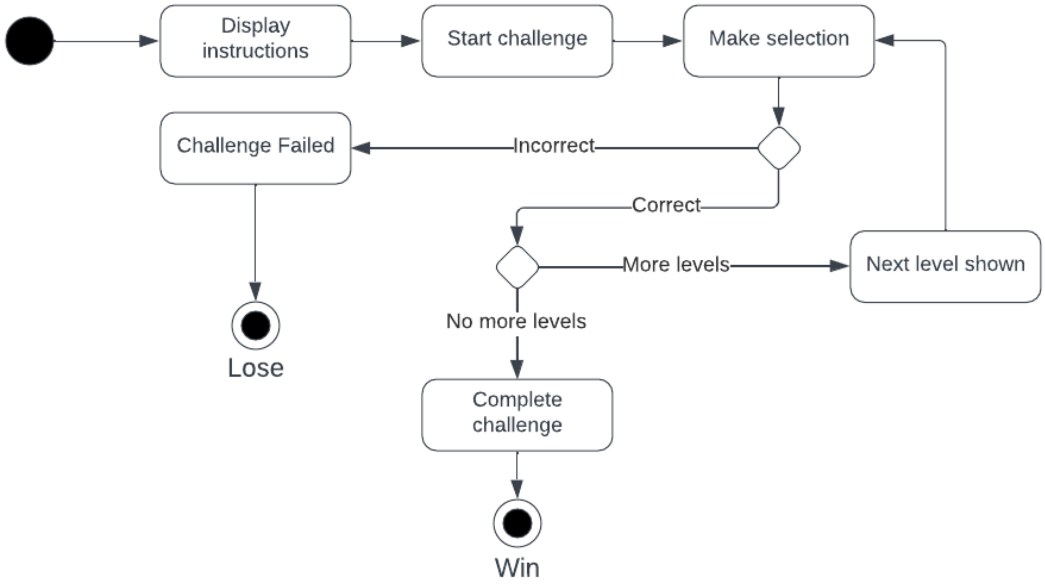


FIGURE 5.9: Activity Diagram: Challenge

5.3 MDA Framework Integration

Application of the MDA framework requires understanding the desired mechanics, dynamics, and aesthetics of the game and how they link together. The framework can be approached from a designer's viewpoint (mechanics to aesthetics) or from a player's viewpoint (aesthetics to mechanics). In the educational game, emphasising a player-experience-driven design, this section will discuss the framework implementation beginning from aesthetics [16].

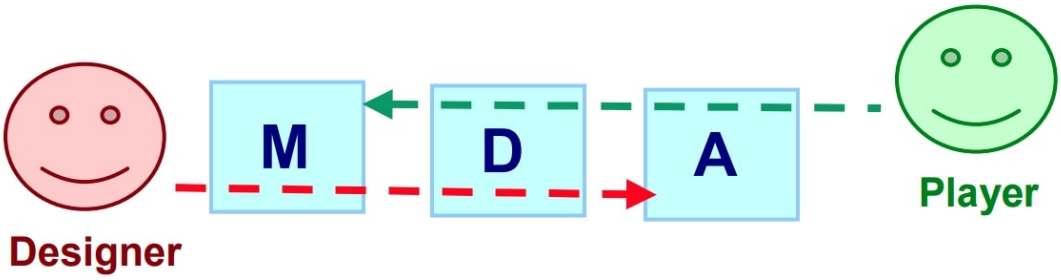


FIGURE 5.10: MDA Framework [16]

5.3.1 Aesthetics

The aesthetic goals of the game should revolve around the emotional responses experienced by the player. From the octalysis review, it was identified that **Accomplishment**, **Empowerment**, and **Social Influence** were predominant motivators [15], [19], [20]. This can be integrated into the list of words described by Hunicke et al, where the main aesthetic objectives will focus on **Challenge** and **Discovery**.

5.3.2 Dynamics

The dynamics are what create our aesthetic experiences [16]. These are the behaviours and interactions resulting from the mechanics. Although the focus is on Challenge and Discovery, other emotions will also be evoked such as Accomplishment and Empowerment but will not be listed.

The dynamics are as follows:

- Challenge
    1. Cybersecurity challenges that require the player to overcome to progress within the escape room.
    2. Time-sensitive challenges.
    3. Elapsed timer for the overall game.
    4. Some major finale
- Discovery
    4. Multiple rooms requiring the player to explore and interact.
    5. Players discover information about different types of scams and how to recognise and avoid them.
    6. Resources used to discover hidden or previously locked locations/objects.
    7. As players progress, they uncover the backstory of the game world.

5.3.3 Mechanics

Mechanics are the fundamental rules and components which will support our gameplay dynamics, affecting the player experience [16].

The mechanics are as follows:

- Navigate room
- Door interaction
- Object interaction
- Challenge timer
- Use resource
- Life system
- Challenge initiation
- Phishing challenge
  - Accept/Reject Letter
- Romance and friendship scam challenge
  - Choose dialogue response
- Password workshop
  - Input password
  - Submit password complying with rules
- Strong password identifier challenge
- Bad policy identifier challenge
- Scareware pop-up challenge
  - Navigate the pop-up
- Complete a challenge
- Collect resource
- Use resource
- Escape room
- Display players results
- Leaderboard of top times

5.3.4 Theme of the game

The theme of the game plays a crucial role in shaping the player experience, aiming for immersion and coherence. Rather than replicating real-world settings, the decision was made to immerse players in a dungeon-esque environment, enhancing the sense of mystery and adventure.

To fully embrace the dungeon-esque theme, various adaptations and modifications are incorporated into the game design process. These include changes in visual aesthetics, resources (such as transitioning from emails to letters), game mechanics, and narrative elements.

Chapter 6

Implementation

The game's implementation is facilitated by Unity, chosen for its versatility and robust feature set. Unity enables us to create immersive environments and implement complex game mechanics effortlessly. Additionally, Unity's supportive community provides access to valuable resources, tutorials, and plugins, enhancing our development process. In the following sections, we'll explore the implementation process and the final game development.

6.1 Gameplay

The gameplay section delves into the interactive elements and challenges that players encounter throughout their playthrough. The player will be able to navigate a menu and explore different escape rooms with varying cyber security challenges.

6.1.1 Instructions

Before the game is started and preceding each challenge, players are presented with instructions guiding them on how to play and tips on what is required from the player. These instructions encompass movement controls and detailed guidelines on navigating through each challenge.

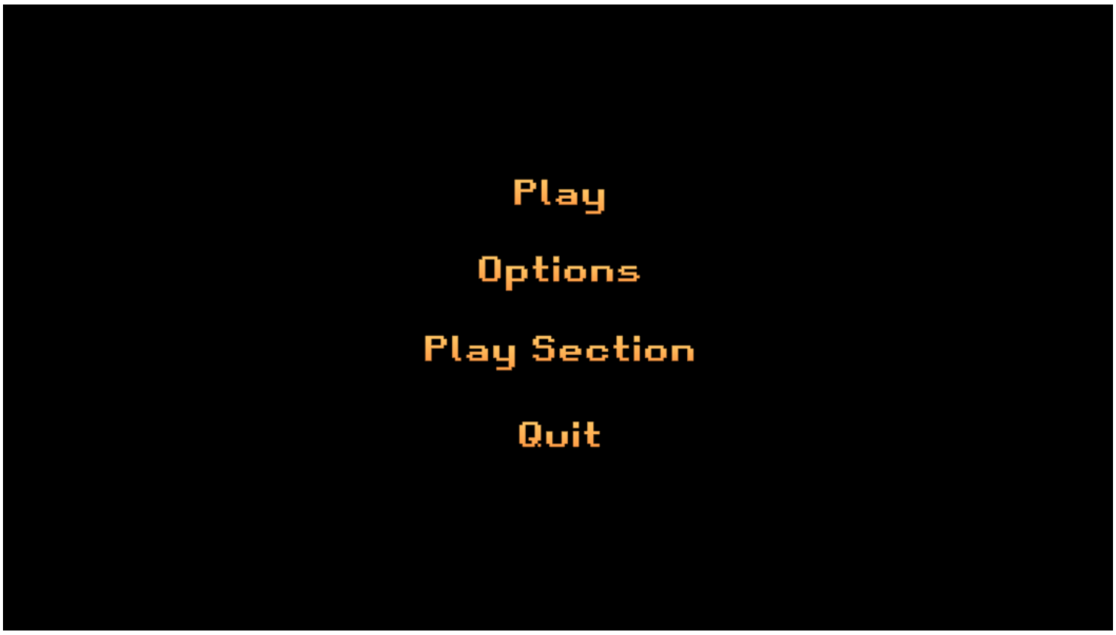


Figure 6.1: Main Menu

6.1.2 Main Menu

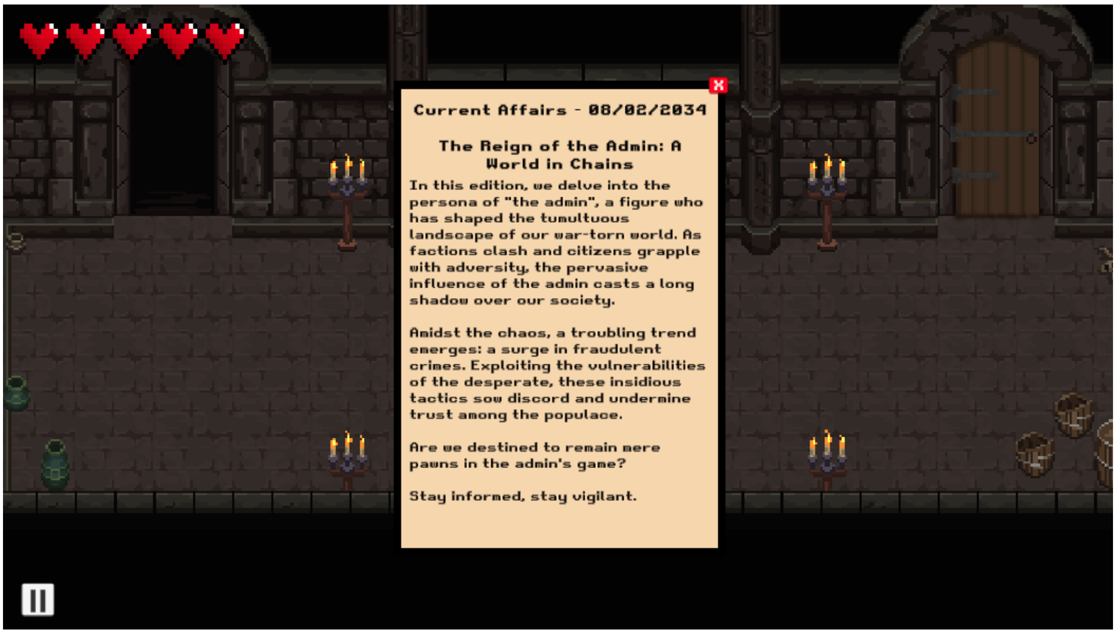
The main menu serves as the player's entry point into the game, providing the ability to start a new game, start at a specific section, and exit the game (Figure 6.1). The ability to configure settings was intended to be added but time constraints led to it being missed.

6.1.3 Escape Room 1 - Introduction

Escape Room 1 serves as the introductory level, where players are introduced to the game world and basic mechanics (Figure 6.2). The environment is designed to familiarise players with navigation controls and interaction methods while setting the stage for the cyber security challenges that lie ahead.

6.1.4 Escape Room 2 - Phishing

Escape Room 2 presents players with a phishing challenge. Instead of emails and links, they encounter deceptive letters and invitations aligning with the game's theme. Corresponding to typical phishing email characteristics [3]–[5], these letters attempt to pose as familiar entities to solicit personal information. To navigate



Current Affairs - 08/02/2034

The Reign of the Admin: A World in Chains

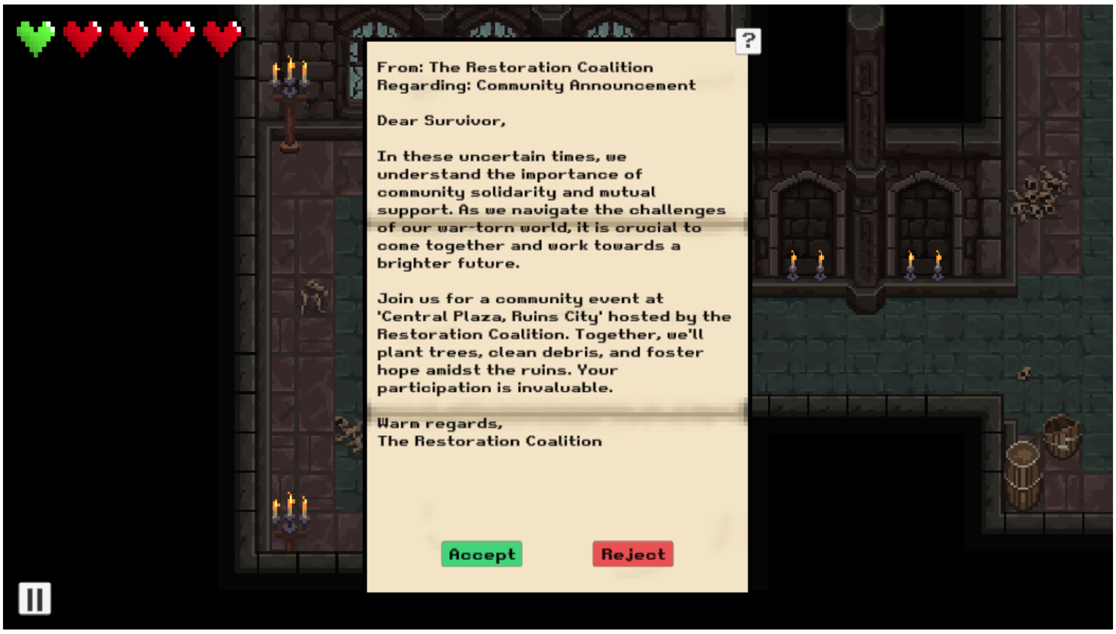
In this edition, we delve into the persona of "the admin", a figure who has shaped the tumultuous landscape of our war-torn world. As factions clash and citizens grapple with adversity, the pervasive influence of the admin casts a long shadow over our society.

Amidst the chaos, a troubling trend emerges: a surge in fraudulent crimes. Exploiting the vulnerabilities of the desperate, these insidious tactics sow discord and undermine trust among the populace.

Are we destined to remain mere pawns in the admin's game?

Stay informed, stay vigilant.

Figure 6.2: Escape Room 1 - Introduction



From: The Restoration Coalition
Regarding: Community Announcement

Dear Survivor,

In these uncertain times, we understand the importance of community solidarity and mutual support. As we navigate the challenges of our war-torn world, it is crucial to come together and work towards a brighter future.

Join us for a community event at 'Central Plaza, Ruins City' hosted by the Restoration Coalition. Together, we'll plant trees, clean debris, and foster hope amidst the ruins. Your participation is invaluable.

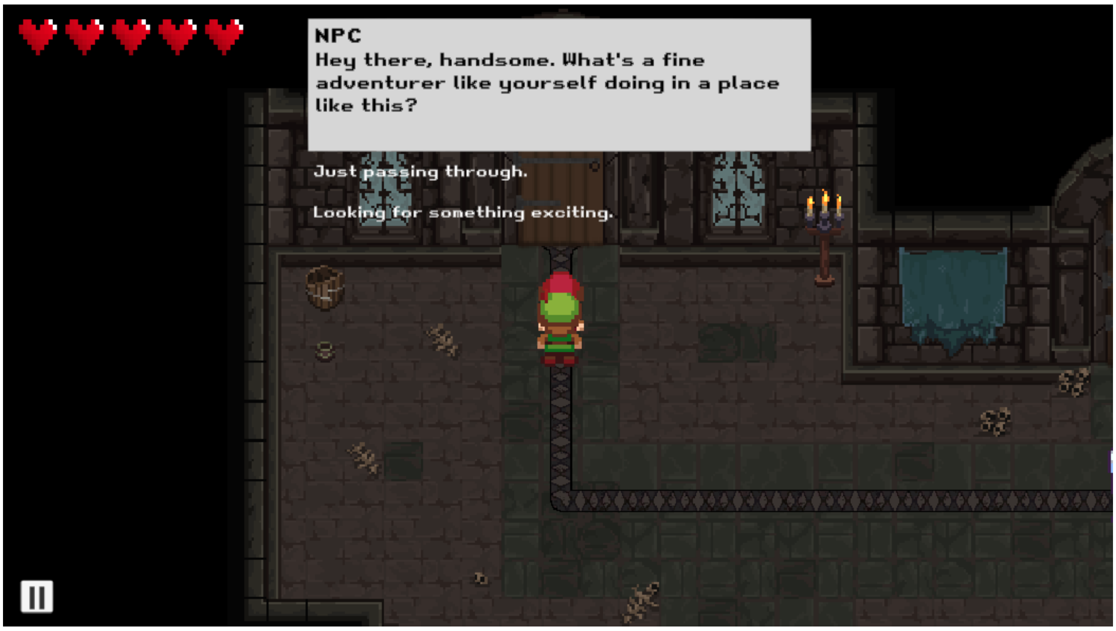
Warm regards,
The Restoration Coalition

Figure 6.3: Escape Room 2 - Phishing

this challenge, players must discern the authenticity of each letter and decide whether to 'Accept' or 'Reject' them (Figure 6.3).

6.1.5 Escape Room 3 - Romance and Friendship Scams

Escape Room 3 delves in romance and friendship scams, presenting players with two dialogue-based challenges featuring Non-Player Characters (NPCs) designed



NPC
Hey there, handsome. What's a fine adventurer like yourself doing in a place like this?

Just passing through.

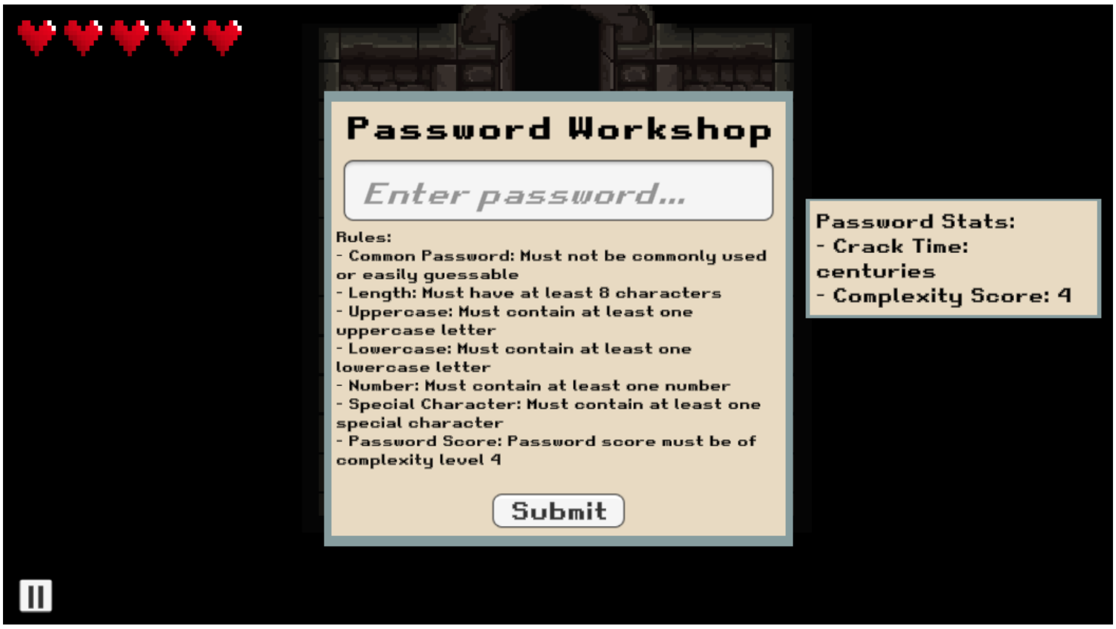
Looking for something exciting.

FIGURE 6.4: Escape Room 3 - Romance and Friendship Scams

to replicate real-life interactions with potential scammers (Figure 6.4). Similar to the reports from Lloyds Bank[5] and the case of 'Zainab'[6], these dialogues aim to deceive players into trusting the NPCs and providing them with assistance. Players are restricted to communicating through preset response options, with one deemed 'safe' and the other 'risky'. To succeed, players must navigate the conversations adeptly, avoiding risky choices and completing the challenge unscathed. The player still has the ability to pass the challenge even after selecting a risky choice as long as the final response does not involve players complying with the NPC's desires.

6.1.6 Escape Room 3.5A - Password Workshop

Escape Room 3.5A focuses on strengthening user passwords with a password workshop. Players are required to create passwords iteratively that adhere to the displayed rules (Figure 6.5). There are 8 essential stages to this challenge. Stage 1 requires the player to enter any password they like, with each proceeding stage adding a new rule which the player needs to adhere to. These rules are comprised of practices that increase the complexity of passwords. As well as this, 'zxcvbn' [10] was utilised in the last rule requiring a complexity level of 4, and to provide an estimated crack time and complexity score on the "Password Stats" window on the right.



Rules:
- Common Password: Must not be commonly used or easily guessable
- Length: Must have at least 8 characters
- Uppercase: Must contain at least one uppercase letter
- Lowercase: Must contain at least one lowercase letter
- Number: Must contain at least one number
- Special Character: Must contain at least one special character
- Password Score: Password score must be of complexity level 4

Password Stats:
- Crack Time: centuries
- Complexity Score: 4

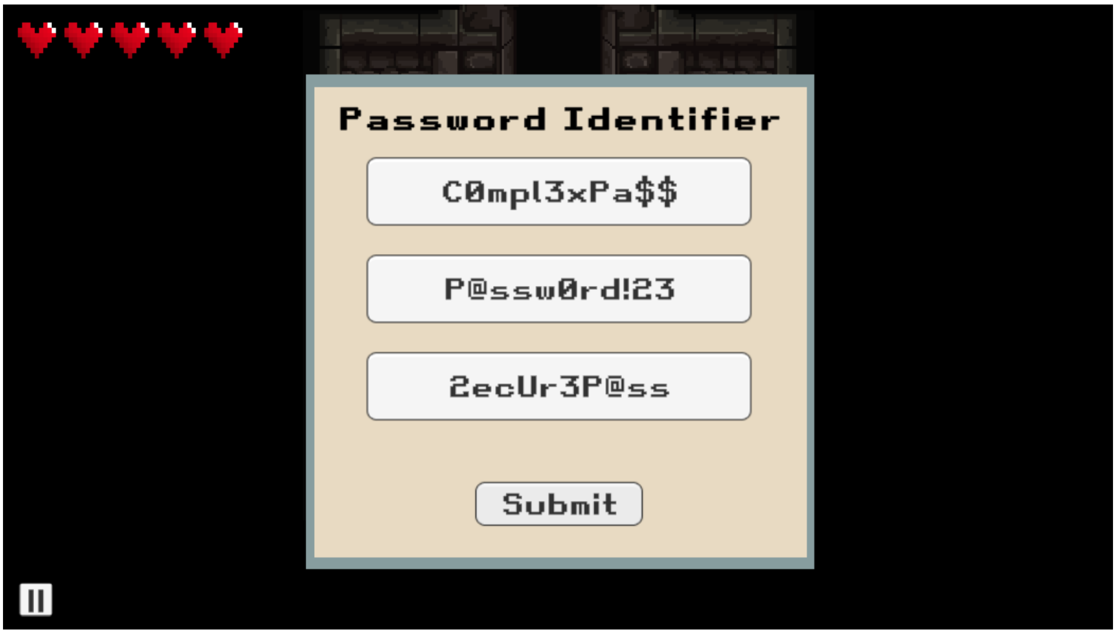
FIGURE 6.5: Escape Room 3.5A - Password Security

6.1.7 Escape Room 3.5B - Strong Password Identifier

Building upon the concepts introduced in Escape Room 3.5A, Escape Room 3.5B presents players with the challenge of identifying the strongest password from a list of options (Figure 6.6). Players must apply their knowledge of password security fundamentals to assess the strength of each password and choose the most robust one. Critical factors include the incorporation of replacement characters (e.g. '@' for 'a') and complexity achieved through factors like length, upper and lower cases, symbols, and numbers. Once again, the 'zxcvbn' tool [10] assists in evaluating each password's complexity to determine the most secure option in each set. Balancing the complexity of passwords was essential to ensure the game remains challenging without becoming overly difficult.

6.1.8 Escape Room 4 - Cyber Policies

Escape Room 4 concludes with a final boss battle against "The Admin". To attack the boss, players must collect an item which enables them to take part in a challenge where they identify the flawed cyber security policy from a set of options (Figure 6.7). Effective policies must be tailored to individual users' needs [11]. However, creating personalised policies for each player would be impractical, requiring extensive customisation for every individual. As a compromise, the game



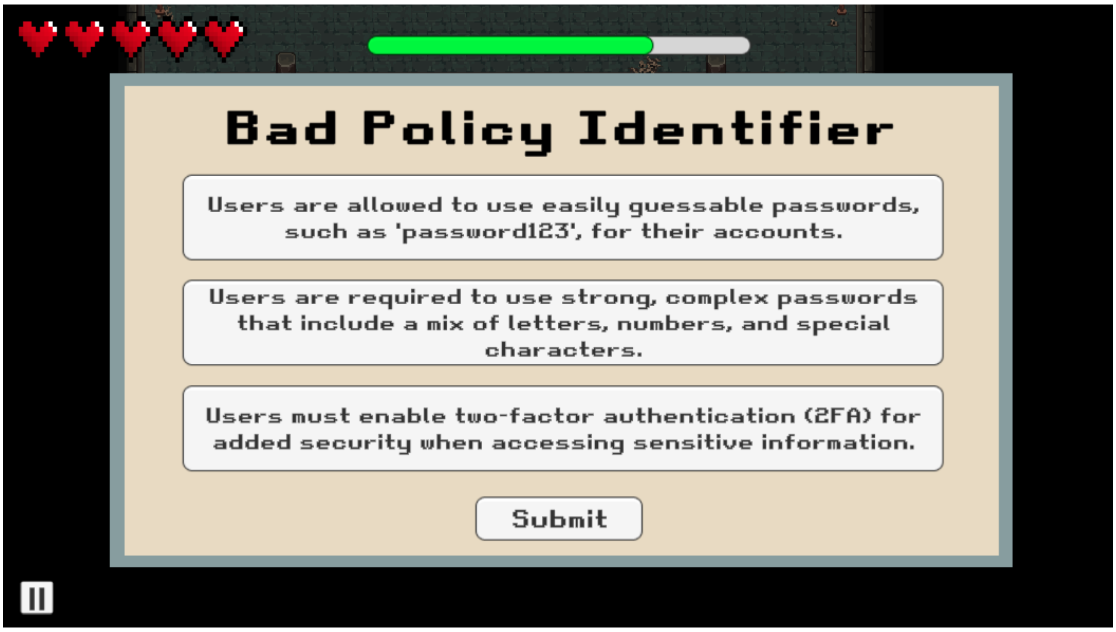
Password Identifier

C0mpl3xPa$$

P@ssw0rd!23

2ecUr3P@ss

FIGURE 6.6: Escape Room 3.5B - Password Security



Bad Policy Identifier

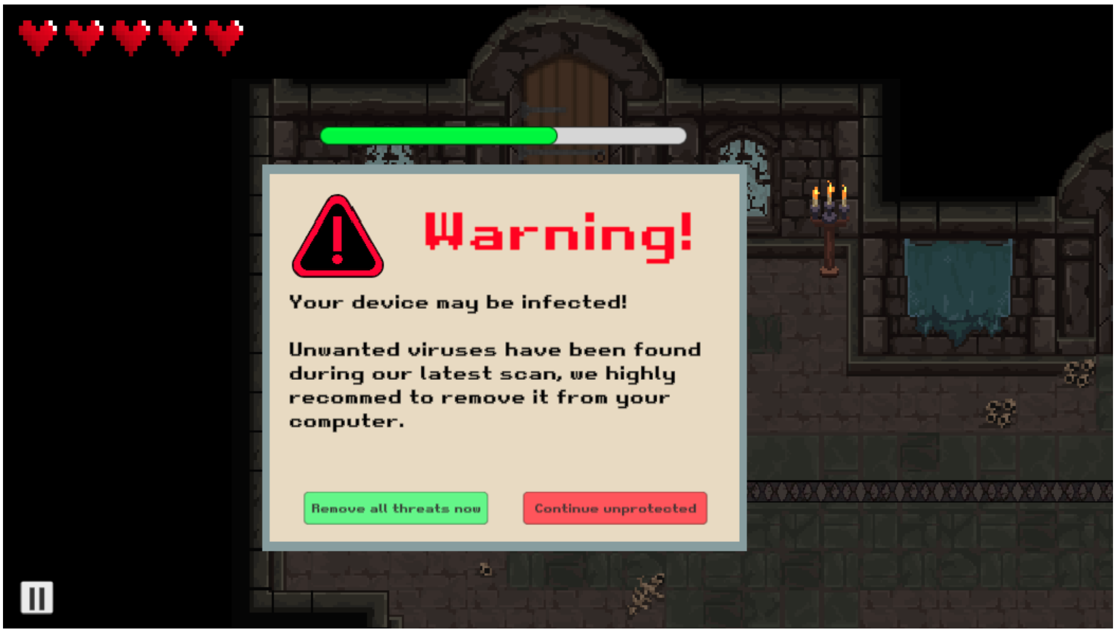
Users are allowed to use easily guessable passwords, such as 'password123', for their accounts.

Users are required to use strong, complex passwords that include a mix of letters, numbers, and special characters.

Users must enable two-factor authentication (2FA) for added security when accessing sensitive information.

FIGURE 6.7: Escape Room 4 - Cyber Policies

presents standardised and overarching policies, highlighting fundamental guidelines that apply universally. Each challenge features a timer to prompt players to make swift decisions, fostering an understanding of characteristics of poor policies.



Warning!

Your device may be infected!

Unwanted viruses have been found during our latest scan, we highly recommed to remove it from your computer.

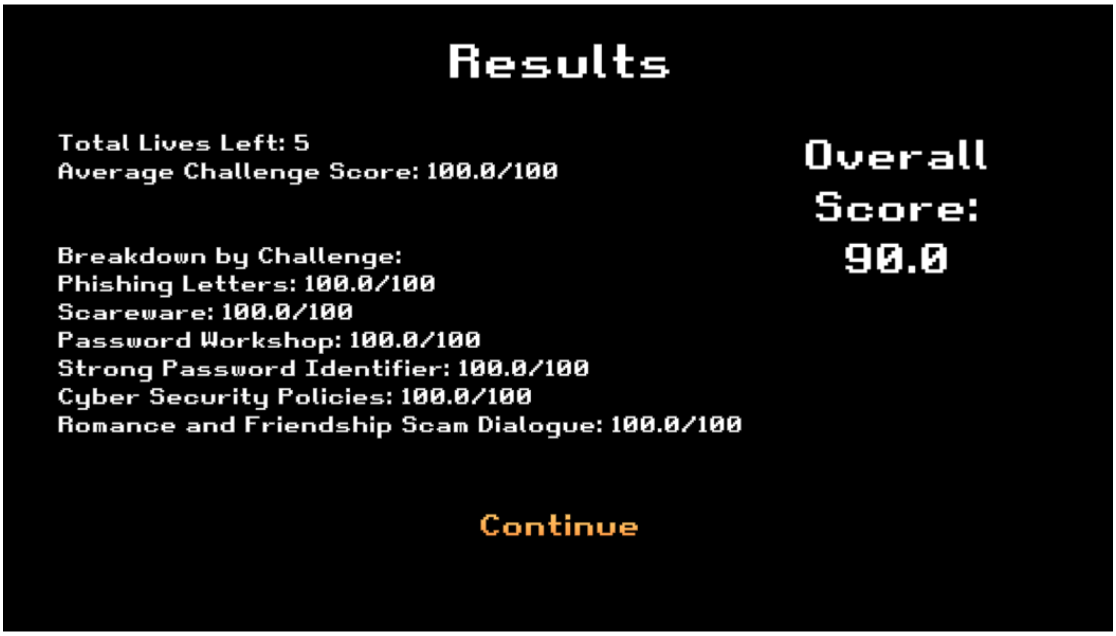
Figure 6.8: Scareware Pop-ups

6.1.9 Scareware Pop-ups

Throughout the game, players will encounter scareware pop-ups designed to mimic real life scenarios (Figure 6.8). These pop-ups aim to manipulate players through false alarms, promises of rewards, and threats. The challenge objective is to deceive the user, compelling them to carefully analyse each pop-up. Variations in the pop-ups require players to pay close attention; for instance, one pop-up may lack an explicit 'safe' button, instead providing instructions within its lengthy description. Accompanied by a timer, each pop-up instils a sense of urgency, heightening the pressure on the player's decision-making process.

6.1.10 Results Screen

Upon defeating the final boss, players are presented with a results screen that provides feedback on their performance throughout the escape rooms (Figure 6.9). This includes their accuracy in each challenge and an overall score calculated from the averages across each challenge and their remaining lives. The results screen serves as a valuable tool allowing players to reflect on their strengths and areas for improvement in cyber security awareness.



Results

Total Lives Left: 5
Average Challenge Score: 100.0/100

Breakdown by Challenge:
Phishing Letters: 100.0/100
Scareware: 100.0/100
Password Workshop: 100.0/100
Strong Password Identifier: 100.0/100
Cyber Security Policies: 100.0/100
Romance and Friendship Scam Dialogue: 100.0/100

Overall Score: 90.0

Figure 6.9: Results Screen

6.2 Core Gameplay Mechanics

To establish the core gameplay experience, it's essential to define key elements such as player interaction, inventory management, the life system, and final score calculation. The following section discusses the significance of each of these components and their operational mechanisms within the game, focusing on conceptual understanding rather than the direct code implementations.

6.2.1 Player Movement and Interactions

To ensure familiarity, standardised controls were utilised. To control the player, the 'WASD' keys are used. Ensuring the player has the ability to interact with objects is crucial for engagement and progression. To interact with objects, the 'E' key was used. Using collision objects, the player is able to start challenges, progress to different rooms, and converse with NPCs.

6.2.2 Inventory

Typically, upon completing a challenge, players a rewarded with a key necessary to unlock a door leading to the next room. These keys are visually represented in the inventory section located at the top right corner of the screen (Figure 6.10).

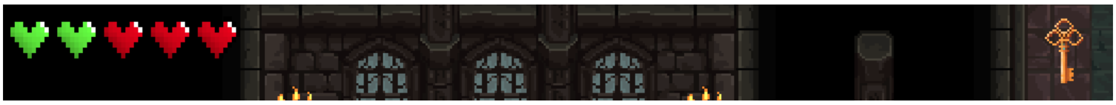


Figure 6.10: UI components showing 7 lives and a key in the inventory

It's worth noting that players can hold multiple keys simultaneously, with each key corresponding to a different door within the environment.

6.2.3 Life System

The life system serves as the way for the player to fail the game. These lives are visually represented in the lives section located at the top left corner of the screen (Figure 6.10). Players start with 5 lives, with 10 lives being the maximum attainable. Losing all lives results in the termination of the game. Mistakes and failures in challenges, and damage taken from the final boss all contribute to the depletion of lives. However, players have the opportunity to replenish their life count through scareware pop-ups (Figure 6.8). Successfully navigating these pop-ups rewards players with an additional life. To prevent cluttering the user interface, any lives beyond the default 5 are represented as green hearts.

6.2.4 Final Score Calculation

After defeating the final boss, players are presented with a results screen (Figure 6.9). This screen provides detailed statistics regarding the player's playthrough, including the number of remaining lives and the score achieved for each challenge.

The score for each challenge ($S_{\text{challenge}}$) is calculated using the formula:

$$S_{\text{challenge}} = \frac{\text{Total Correct Answers}}{\text{Total Attempts}} \times 100$$

where:

- Total Correct Answers represents the sum of correct answers obtained in the final attempt.
- Total Attempts represents the sum of correct answers in the final attempt, as well as every incorrect answer across all attempts.

The overall score (S_{overall}) is determined by combining two key factors: the number of remaining lives (L) and the average challenge score (S_{avg}). The calculation is performed as follows:

$$S_{\text{overall}} = (W_{\text{lives}} \times \frac{\text{Remaining Lives}}{\text{Total Lives}} \times 100) + (W_{\text{challenges}} \times S_{\text{avg}})$$

where:

- W_{lives} represents the weight assigned to the remaining lives, set at 20%.
- $W_{\text{challenges}}$ denotes the weight assigned to the average challenge score, set at 80%.
- Remaining Lives signifies the number of remaining lives out of a possible maximum of 10.
- Total Lives represents the maximum possible number of lives, which is 10.
- S_{avg} represents the average score achieved across all challenges.

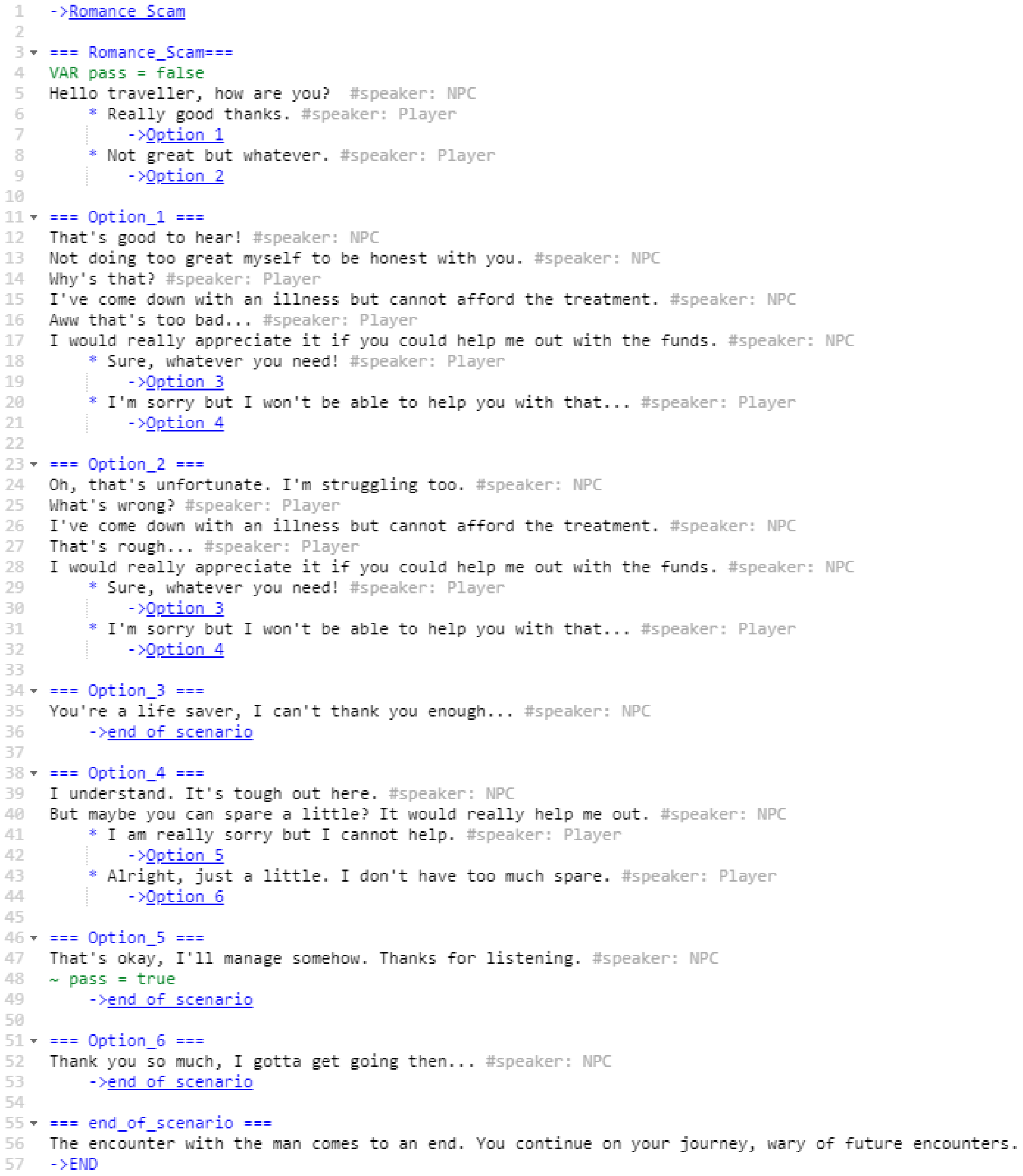
By presenting a results scene, players receive immediate feedback on their performance, offering insights into their strengths and weaknesses. This feedback not only serves as a motivational tool but also facilitates self-assessment and improvement. Striving for a perfect score of 100 becomes a tangible goal, driving players to master each cyber security concept and enhance their overall gameplay experience.

6.3 Assets

While some assets have been created in Photoshop, the majority of the game is built from assets from the Unity and Itch.io asset stores.

6.4 Tools and Plugins

Third party tools and plugins were also used to assist in development. These include ink, zxcvbn, and a predeveloped A* pathfinding solution. By utilising established plugins and tools, we can guarantee a higher level of reliability and stability as these have already been tested and optimised by developers.



```
->Romance_Scam

=== Romance_Scam===
VAR pass = false
Hello traveller, how are you?  #speaker: NPC
    * Really good thanks. #speaker: Player
        ->Option_1
    * Not great but whatever. #speaker: Player
        ->Option_2

=== Option_1 ===
That's good to hear! #speaker: NPC
Not doing too great myself to be honest with you. #speaker: NPC
Why's that? #speaker: Player
I've come down with an illness but cannot afford the treatment. #speaker: NPC
Aww that's too bad... #speaker: Player
I would really appreciate it if you could help me out with the funds. #speaker: NPC
    * Sure, whatever you need! #speaker: Player
        ->Option_3
    * I'm sorry but I won't be able to help you with that... #speaker: Player
        ->Option_4

=== Option_2 ===
Oh, that's unfortunate. I'm struggling too. #speaker: NPC
What's wrong? #speaker: Player
I've come down with an illness but cannot afford the treatment. #speaker: NPC
That's rough... #speaker: Player
I would really appreciate it if you could help me out with the funds. #speaker: NPC
    * Sure, whatever you need! #speaker: Player
        ->Option_3
    * I'm sorry but I won't be able to help you with that... #speaker: Player
        ->Option_4

=== Option_3 ===
You're a life saver, I can't thank you enough... #speaker: NPC
    ->end_of_scenario

=== Option_4 ===
I understand. It's tough out here. #speaker: NPC
But maybe you can spare a little? It would really help me out. #speaker: NPC
    * I am really sorry but I cannot help. #speaker: Player
        ->Option_5
    * Alright, just a little. I don't have too much spare. #speaker: Player
        ->Option_6

=== Option_5 ===
That's okay, I'll manage somehow. Thanks for listening. #speaker: NPC
~ pass = true
    ->end_of_scenario

=== Option_6 ===
Thank you so much, I gotta get going then... #speaker: NPC
    ->end_of_scenario

=== end_of_scenario ===
The encounter with the man comes to an end. You continue on your journey, wary of future encounters.
->END
```

Figure 6.11: ink Dialogue of NPC 2 (ScamGame2.ink)

6.4.1 ink

ink is a narrative scripting language used for games. Acting as middleware for Unity, ink allowed for simple creation of the dialogues present in the game. The language also provided the ability to implement diversions, choices, and variables which was essential in the NPC dialogue conversations as seen in Figure 6.4. Figure 6.11 shows the script of an NPC. A variable '*pass*' was used to represent whether the player has made the correct choices. Response choices were used to divert to different dialogue paths leading to the players success or failure.

6.4.2 zxcvbn

zxcvbn is a password strength estimation library developed by Dropbox utilising pattern matching and estimation [10]. In essence, zxcvbn identifies weak passwords by comparing them to dictionaries of common words and detecting weak character replacements (such as 'a' to '@'). While many applications only consider basic requirements such as length, uppercase, and numbers, Zxcvbn provides a more comprehensive evaluation of password security.

In the game, zxcvbn was utilised in both of the password challenges as seen in Figures 6.5 and 6.6. In the password workshop, Zxcvbn actively calculated crack times and complexity scores for each user input. In the strong password identifier challenge zxcvbn was used to decide which of the displayed passwords was the most complex. Although the dictionary functionality was intended to be utilised, WebGL restrictions were encountered that prevented us from loading external files within the game build for security reasons. Consequently, this feature had to be abandoned as a suitable alternative could not be found.

6.4.3 A* Pathfinding

For the final boss fight, the Ultimate A* Pathfinding Solution plugin from the Unity asset store was used. A* is a widely-used pathfinding algorithm known for its efficiency in finding the shortest path between two nodes. Utilising the capabilities of the plugin, the A* algorithm was seamlessly integrated into the boss' AI system. Figure 6.12 showcases an example path generated by the algorithm for the boss AI. The boss AI will generate the shortest path to the player and will only generate a new path once it has reached its destination.

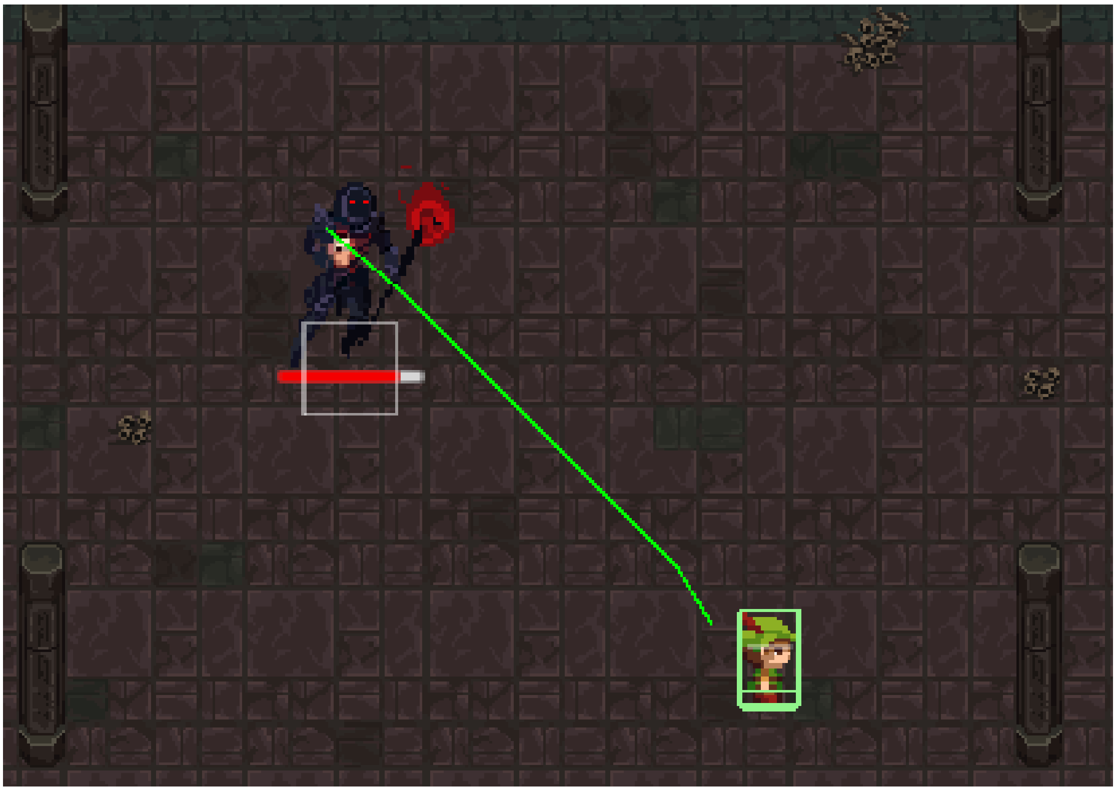


Figure 6.12: A* Algorithm example path for the boss AI

Chapter 7

Testing and Evaluation

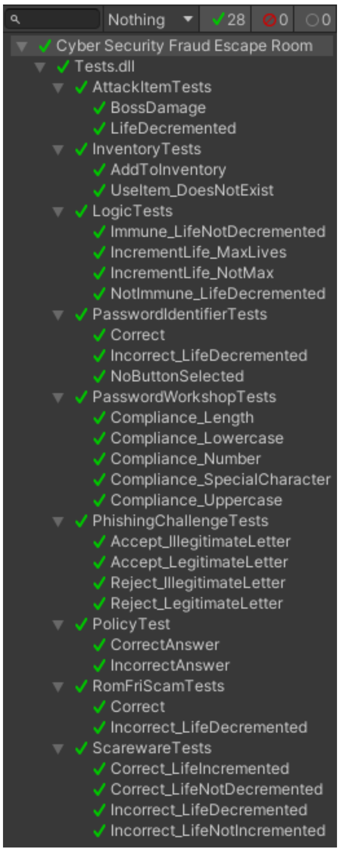
To ensure a fully functioning game, both unit testing and functional testing were crucial components for validating specific aspects of the game's performance. These tests also served to confirm if the requirements outlined in Table 4.2 were met. Additionally, user testing was conducted to asses the game's effectiveness in teaching cybersecurity concepts.

7.1 Unit Testing

Unit testing involves testing individual units or components of software to ensure they meet expectations. Due to immature knowledge of Unity, writing unit testable code became increasingly more difficult as the project expanded. Consequently, only basic unit tests were performed which focused on essential gameplay elements. These tests scrutinised functionalities like inventory and logic management, along with individual challenges to verify proper life adjustments and stage progression, as depicted in Figure 7.1

7.2 Functional Testing

Functional testing involved testing the game's overall behaviour against the specified requirements outlined in the Requirements Analysis phase (Table 4.2 and Table 4.3). The testing process involved a systematic evaluation of each requirement to determine its fulfilment. This evaluation involved the execution of various



```
Nothing ▾   ✓28   ⊘0   ○0
▼ ✓ Cyber Security Fraud Escape Room
  ▼ ✓ Tests.dll
    ▼ ✓ AttackItemTests
        ✓ BossDamage
        ✓ LifeDecremented
    ▼ ✓ InventoryTests
        ✓ AddToInventory
        ✓ UseItem_DoesNotExist
    ▼ ✓ LogicTests
        ✓ Immune_LifeNotDecremented
        ✓ IncrementLife_MaxLives
        ✓ IncrementLife_NotMax
        ✓ NotImmune_LifeDecremented
    ▼ ✓ PasswordIdentifierTests
        ✓ Correct
        ✓ Incorrect_LifeDecremented
        ✓ NoButtonSelected
    ▼ ✓ PasswordWorkshopTests
        ✓ Compliance_Length
        ✓ Compliance_Lowercase
        ✓ Compliance_Number
        ✓ Compliance_SpecialCharacter
        ✓ Compliance_Uppercase
    ▼ ✓ PhishingChallengeTests
        ✓ Accept_IllegitimateLetter
        ✓ Accept_LegitimateLetter
        ✓ Reject_IllegitimateLetter
        ✓ Reject_LegitimateLetter
    ▼ ✓ PolicyTest
        ✓ CorrectAnswer
        ✓ IncorrectAnswer
    ▼ ✓ RomFriScamTests
        ✓ Correct
        ✓ Incorrect_LifeDecremented
    ▼ ✓ ScarewareTests
        ✓ Correct_LifeIncremented
        ✓ Correct_LifeNotDecremented
        ✓ Incorrect_LifeDecremented
        ✓ Incorrect_LifeNotIncremented
```

Figure 7.1: Unity Test Runner

scenarios and interactions within the game to validate its behaviour against the defined criteria. Notably, the tests were conducted upon each new implementation/adjustment of a functionality. These tests were primarily conducted on prototype builds due to performance disparities between the Unity editor and the final builds.

7.3 User Testing

To assess the game's effectiveness as an educational tool, a questionnaire was created and shared across various social medias and forums. Participants were asked about their understanding of their knowledge before playing the game, their knowledge after playing the game, as well as various bugs and improvements which could be implemented.

The requirements of ERGO/FEPS/92262 were followed.

7.3.1 Participant Demographic

Before delving into the evaluation results, it's important to understand the demographic of the participants involved in the testing phase. In total, 12 participants took part in the questionnaire.

The age range of the participants spanned from 18 to 25. All participants reported being familiar with the use of technology and the majority of them at least somewhat familiar with cybersecurity concepts. While it would have been beneficial to have a more diverse representation of participants with varying levels of familiarity with cybersecurity concepts, constraints such as time limitations and the format of the study may have impacted recruitment efforts.

Table 7.1: Technology and Cybersecurity familiarity results

	Technology?	**Cybersecurity concepts?**
Not at all familiar	0	1
Moderately familiar	0	7
Very familiar	12	4

7.3.2 Pre- and Post-Game Knowledge Levels

Before playing the game, participants' knowledge levels across the relevant topics were asked. Post-game, the participant's knowledge levels were re-evaluated to measure the impact of the game on their understanding. These levels were assessed on a scale from 1-5 with 1 being no understanding and 5 being an expert understanding. Figure 7.2 shows the average before and after knowledge ratings of all participants across all the topics. Overall, participants showed an increase in their perceived understanding as can be seen in the shift in the distribution towards to right side. As shown in Table 7.2, each individual topic found an improvement in knowledge with the most notable improvements seen in Cyber Policies and Scareware.

Participant's knowledge levels across different categories were analysed to understand what type of person is most effected. In the initial questions, participants were asked about their current familiarity with cybersecurity concepts. Using this information, participants were categorised into 3 groups; Level 1 (Not at all familiar), Level 2 (Moderately familiar), and Level 3 (Very familiar). The average increases in knowledge levels 1,2, and 3 are presented in Table 7.3.

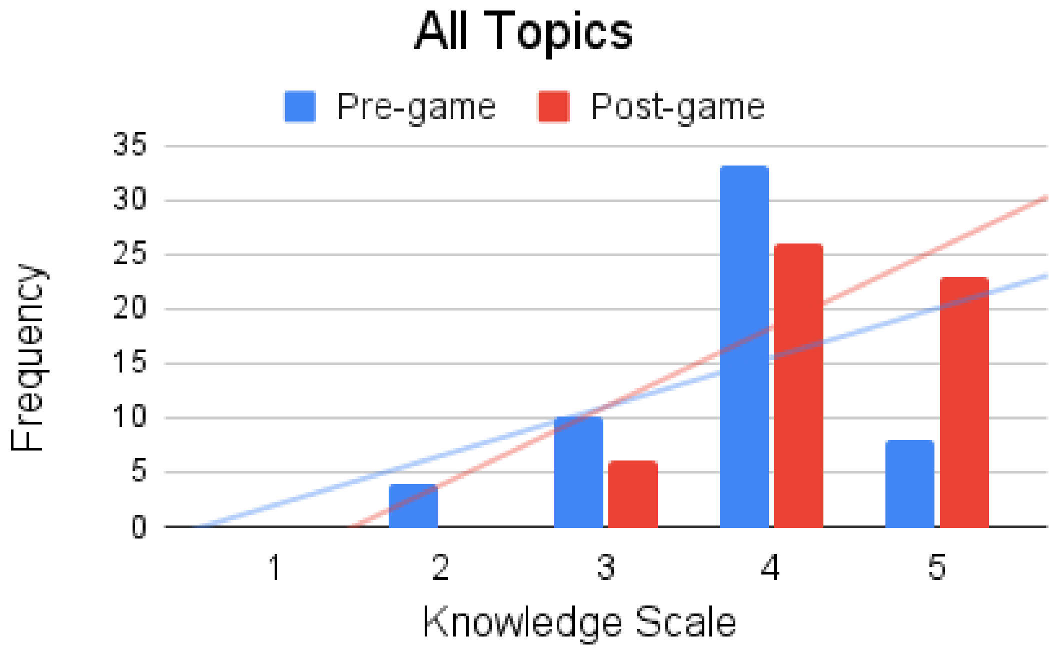


Figure 7.2: Average Knowledge Ratings across all Topics

Table 7.2: Pre- and Post-Game Knowledge Levels

Topic	**Pre-game (/5)**	**Post-game (/5)**	**%Difference Pre and Post**
Phishing	3.82	4.18	9.52%
R&F Scams	3.91	4.18	6.98%
Password Security	4.18	4.36	4.35%
Cyber Policies	3.64	4.36	20.00%
Scareware	3.55	4.45	25.64%
All	3.82	4.31	13.30%

Level 3 participants showed relatively smaller increases in knowledge compared to Levels 1 and 2. This can be attributed to their initial high level of familiarity with cybersecurity concepts. On the other hand, Level 1 participant who initially had no familiarity with cybersecurity concepts, showed significant increases in knowledge. It's worth noting that only one participant fell into Level 1, which heavily limited the generalisability of findings for this group. Level 2 participants exhibited increases in knowledge that were likely the most accurate reflections of the effectiveness of the training game due to the larger number of participants and large potential for improvement.

Table 7.3: Knowledge Level Increases

Topic	Level 1 Average Increase	Level 2 Average Increase	Level 3 Average Increase
Phishing	2	0.29	0
R&F Scams	0	0.43	0
Password Security	-1	0.43	0
Cyber Policies	1	0.86	0.33
Scareware	2	1.14	0
All	0.80	0.63	0.07

7.3.3 Effectiveness at Teaching and Reinforcing Ideas

Participants rated the effectiveness of the game at teaching and reinforcing cybersecurity concepts. On average, the game was rated 3.83/5 for both teaching and reinforcing, indicating a balanced approach. The teaching versus reinforcing aspect of the game was also evaluated, with participants perceiving the game to be more reinforcing than teaching, as shown in Table 7.4.

Table 7.4: Teaching and Reinforcing Effectiveness

Metric	Rating (/5)
Average Effectiveness at Teaching	3.83
Average Effectiveness at Reinforcing	3.83
Teaching vs Reinforcing (1-5)	3.83

7.3.4 User Engagement and Enjoyment

Participants' engagement and enjoyment levels were assessed to gauge their overall experience with the game. On average, participants found the game to be highly engaging and enjoyable as shown in Table 7.5.

Table 7.5: Engagement and Enjoyment

Metric	Rating (/5)
Average Engagement	3.92
Average Enjoyment	3.83

7.3.5 Gameplay Issues and Improvements

During the testing phase, participants also provided feedback on the gameplay experience. Overall, the interface was found to be intuitive, with no major gameplay issues reported. However, the Knowledge Level 1 participant found the interface to not be user-friendly, highlighting the importance of refining the user interface to ensure a seamless gameplay experience for all users.

7.3.6 Limitations and Considerations

Acknowledging the limitations and considerations that may have influenced the interpretation and generalisability of the findings is essential:

- Sample Size and Representation
  - The study's sample size was relatively small, with only 12 participants. Despite efforts to share the questionnaire across multiple platforms, the nature of the study, requiring participants to engage in gameplay, may have deterred potential participants. This could have introduced a bias toward individuals who are already comfortable with technology and somewhat familiar with cybersecurity concepts.
- Ignored Participant Answers
  - Owing to the small sample size, participant responses carried significant weight in the analysis. Consequently, some responses were disregarded, particularly those indicating a decreased understanding of the topics after playing the game. It's worth noting that participants may have overestimated their initial understanding rather than genuinely experiencing a decrease in knowledge.

7.4 Evaluation

Table 7.6 presents the relevant requirements along with their completion status. The 'Must' labelled requirements were prioritised for implementation to guarantee success. Unmet requirements stemmed from various factors, including time constraints or dependency failures. For instance, the absence of account and leaderboard functionalities (F1, F2, F3) resulted in no need to store user data (NF9). Functional requirements are denoted by 'F', while Non-Functional Requirements are denoted by 'NF'.

Table 7.6: Relevant Functional and Non-Functional Requirements

ID	Requirement	MoSCoW	Completed
F1	Users can create an account	Could	Ignored
F2	Users can login to their account	Could	Ignored
F3	Users can manage their account	Could	Ignored
F4	Users can navigate a user interface	Must	Yes
F5	Users can access learning material for various cybersecurity topics	Should	No
F6	Users can play scenario simulations of attacks	Must	Yes
F7	The game will provide an introduction with instructions for each challenge	Must	Yes
F8	The challenges will have time-limits	Must	Yes
F9	Users can view performance analytics	Should	Yes
F10	The game will provide the user with their strengths and weaknesses	Could	Yes
F11	Users can view a performance leaderboard	Could	No
F12	Users can customise the game visually by increasing font size and changing themes	Should	No
F13	Users can play against others (multiplayer)	Won't	No
F14	Users are rewarded dependent on how well they perform (time, failures)	Must	Yes
F15	Users can customise what content is shown	Could	Yes
F16	Users can receive hints/clues if they are stuck	Could	No
F17	The game will provide an initial tutorial to understand the games mechanics	Must	Yes
F18	Users are punished for failures	Must	Yes
F19	The game will be level based to accommodate for further expansion	Must	Yes
NF1	The game will be responsive	Must	Yes
NF2	The game will not stutter	Must	Yes
NF3	The game should be intuitive	Must	Yes
NF4	The game should be user-friendly	Must	Yes
NF5	The game will provide clear instructions to the user	Must	Yes
NF6	The game will provide guidance to the user	Must	Yes
NF7	The game will be compatible with different devices	Could	No
NF8	The game will be compatible on different operating systems	Could	Yes
NF9	The game will store users data securely	Must	Ignored
NF10	The game will be consistent with accessibility customisations	Should	No
NF11	The game will strengthen their cybersecurity knowledge	Must	Yes
NF12	The game will be relatable to real-life scenarios	Must	Yes

Chapter 8

Project Management

The following section describes the project management including the tools utilised and progression of the project. A risk assessment was also performed to comprehend the various potential risks associated with this project.

8.1 Development Tools and Technologies

Table 8.1 describes the tools and technologies which have been utilised or are to be utilised in the project.

Table 8.1: Tools and Technologies

Tools	Description
GitLab	Project management
Lucid Chart	Online software for UML diagrams
Figma	Create wireframes of the design
Zotero	Reference management software for literature research
Microsoft Teams	Communication software for meetings
C#	Programming language for Unity
Unity	Game engine for game development
Unity Asset Store	Asset store for the Unity engine
Photoshop	Used to design some assets
Itch.io	Website used to host the game and asset store
ink	Narrative scripting language for dialogue
Zxcvbn	Password strength estimator

8.2 Assets used

Below are all the assets used in the making of the game.

2D Pixel Art Icons - Swords
2D Pixel Item Asset Pack
Pixel Art Key Pack - Animated
Rogue Fantasy Castle
Tiny RPG - Forest
Pixel Art Top Down - Basic
Ink Integration for Unity
Ultimate A* Pathfinding Solution
Fantasy RPG Chests
Necromancer
Effect and Bullet
zxcvbn-cs by Dropbox

8.3 Risk Assessment

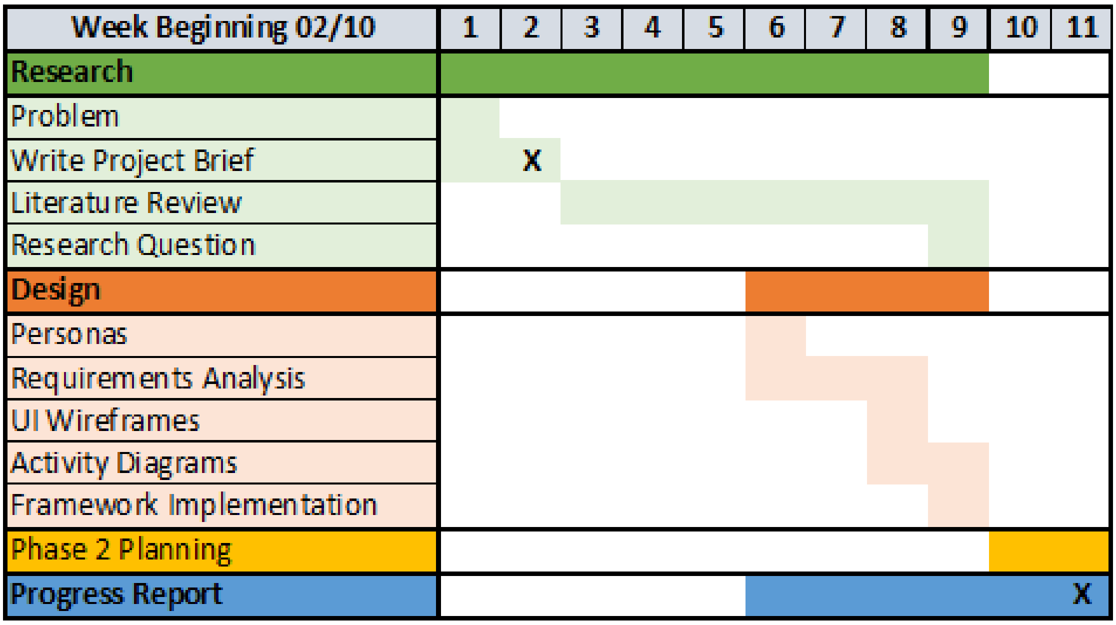
The following risk assessment as shown in Table 8.2 was used to evaluate the potential risks associated with the project. The probability (P) and severity (S) of each risk is estimated to give us the overall risk exposure (RE). The risk assessment identifies mitigation strategies for each risk to minimise or avoid damages.

TABLE 8.2: Risk Assessment

Risk	**P**	**S**	**RE**	**Mitigation**
Project deadline not met	3	5	15	Have weekly meetings with the project supervisor to ensure progress is being made at a good pace
Overly optimistic schedule	3	4	12	Schedule my time and plan the project into smaller iterations
Final project lacks relevancy to the problem	1	5	5	Continuously refer back to the initial problem statement
Application is not educational	3	4	12	Review cybersecurity contents and ensure implementation
Difficulty in transitioning from Java to C#	4	4	16	Allocate learning time for C# and Unity. Utilise online resources and practice
Lack of familiarity with Unity development	4	4	16	Allocate learning time for Unity. Utilise online resources and practice
Data loss	1	5	5	Use Git version control and a local backup
Equipment loss/failure	1	3	3	Replacement equipment available
Illness	1	3	3	Ensure good health practices and schedule rest periods

8.4 Gantt Chart for Phase 1

The schedule for planning and research completed in phase 1 is illustrated in Figure 8.1.

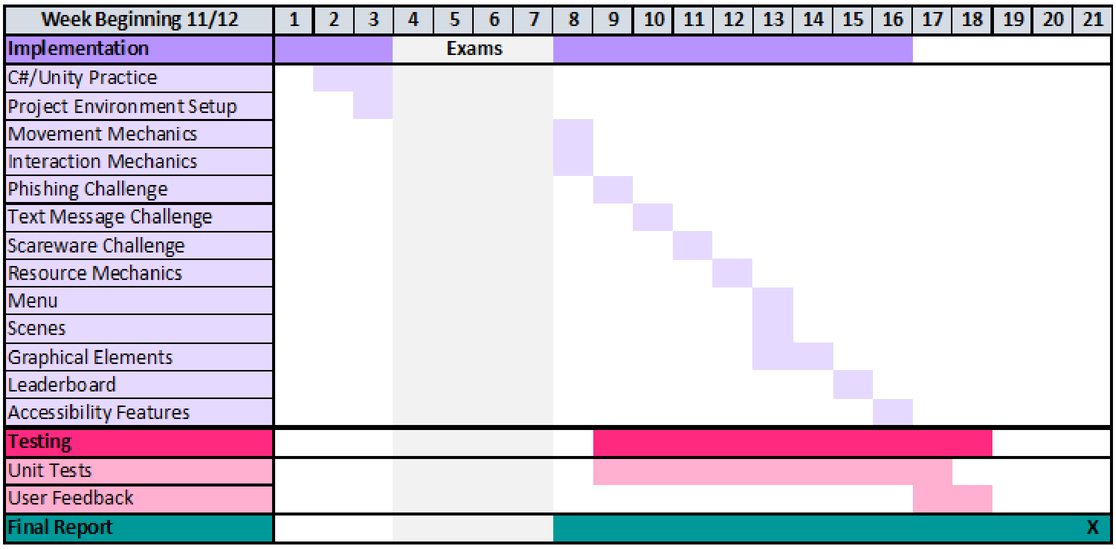


Week Beginning 02/10	1	2	3	4	5	6	7	8	9	10	11
Research	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩		
Problem	🟩										
Write Project Brief	🟩	X									
Literature Review			🟩	🟩	🟩	🟩	🟩	🟩	🟩		
Research Question									🟩		
Design						🟧	🟧	🟧	🟧		
Personas						🟧					
Requirements Analysis						🟧	🟧	🟧			
UI Wireframes								🟧			
Activity Diagrams								🟧	🟧		
Framework Implementation									🟧		
Phase 2 Planning										🟨	🟨
Progress Report						🟦	🟦	🟦	🟦	🟦	X

FIGURE 8.1: Phase 1 Gantt Chart

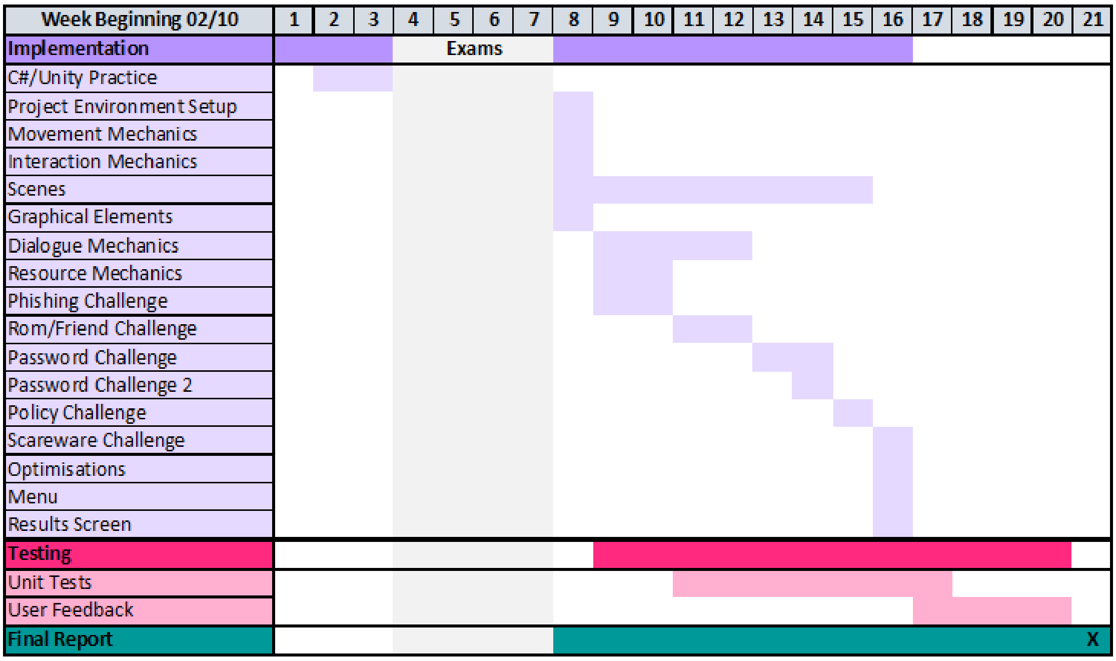
8.5 Gantt Chart for Phase 2

Figure 8.2 presents the proposed schedule for phase 2, while Figure 8.3 displays the actual schedule. Throughout the project's development, additional tasks emerged and were integrated into the actual schedule. In general, the proposed plan remained mostly accurate, although certain tasks took slightly longer than initially anticipated.



Week Beginning 11/12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Implementation	■	■	■	Exams				■	■	■	■	■	■	■	■	■					
C#/Unity Practice		■	■																		
Project Environment Setup			■																		
Movement Mechanics								■													
Interaction Mechanics								■													
Phishing Challenge									■												
Text Message Challenge										■											
Scareware Challenge											■										
Resource Mechanics												■									
Menu													■								
Scenes													■								
Graphical Elements													■	■							
Leaderboard															■						
Accessibility Features																■					
Testing									■	■	■	■	■	■	■	■	■	■			
Unit Tests									■	■	■	■	■	■	■	■	■				
User Feedback																	■	■			
Final Report								■	■	■	■	■	■	■	■	■	■	■	■	■	X

FIGURE 8.2: Expected Phase 2 Gantt Chart



Week Beginning 02/10	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Implementation	■	■	■	Exams				■	■	■	■	■	■	■	■	■					
C#/Unity Practice		■	■																		
Project Environment Setup								■													
Movement Mechanics								■													
Interaction Mechanics								■													
Scenes								■	■	■	■	■	■	■	■						
Graphical Elements								■													
Dialogue Mechanics									■	■	■	■									
Resource Mechanics									■	■											
Phishing Challenge									■	■											
Rom/Friend Challenge											■	■									
Password Challenge													■	■							
Password Challenge 2														■							
Policy Challenge															■						
Scareware Challenge																■					
Optimisations																■					
Menu																■					
Results Screen																■					
Testing									■	■	■	■	■	■	■	■	■	■	■	■	
Unit Tests											■	■	■	■	■	■	■				
User Feedback																	■	■	■	■	
Final Report								■	■	■	■	■	■	■	■	■	■	■	■	■	X

FIGURE 8.3: Actual Phase 2 Gantt Chart

Chapter 9

Conclusion

The prevalence of cyber attacks targeting human vulnerabilities, particularly through techniques like phishing and social engineering, underscores the critical importance of effective cybersecurity education and awareness. This research explored the application of gamification techniques to enhance cybersecurity learning and address the gaps in mitigating human error.

By developing an educational escape room game following the (MDA) framework, this project provided an immersive and engaging approach to teaching core cybersecurity concepts. The game encompassed a range of challenges focused on phishing, romance scams, password security, and cyber policies – all areas where human lapses can introduce vulnerabilities.

Through user testing, the game demonstrated its effectiveness in improving participants' understanding of these cybersecurity topics while maintaining an enjoyable gameplay experience. Notably, participants who initially had limited familiarity with cybersecurity exhibited the most substantial knowledge gains, highlighting the game's potential in raising awareness among less tech-savvy individuals.

However, it is important to acknowledge the study's limitations, including the relatively small sample size and lack of diversity in participant demographics. Further large-scale testing and comparisons against traditional learning methods are necessary to establish the game's effectiveness more conclusively.

9.1 Future Work

There are several potential extensions and improvements that could be considered for future work. Implementing the features listed below could further enhance the user experience and potentially increase its educational value.

- **Enhanced Social Features:** Introducing multiplayer elements or community-driven aspects could further enhance the games engagement and enjoyment. These could include leaderboards, or potentially cooperative challenges.
- **Expanded Content and Scenarios:** Expanding the game's content with new challenges and scenarios could provide greater educational benefit.
- **Accessibility Options:** As part of one the requirements, having the ability to customise font size and themes was discussed. Implementing these options could ensure that a wider population is being accommodated for.
- **Cross-Platform Compatibility:** Enhancing the game's compatibility to allow players to access it across different devices and platforms (e.g. tablets, smartphones) could increase accessibility and reach a wider audience.

Bibliography

[1] M. Alsharif, S. Mishra, and M. Alshehri, "Impact of Human Vulnerabilities on Cybersecurity," *Computer Systems Science and Engineering*, vol. 40, Sep. 28, 2021. DOI: 10.32604/csse.2022.019938.

[2] A. Manzano-León, P. Camacho-Lazarraga, M. A. Guerrero, *et al.*, "Between Level Up and Game Over: A Systematic Literature Review of Gamification in Education," *Sustainability*, vol. 13, no. 4, p. 2247, 4 Feb. 19, 2021, ISSN: 2071-1050. DOI: 10.3390/su13042247.

[3] A. M. Syed, *Social engineering: Concepts, Techniques and Security Countermeasures*, Jun. 23, 2021. DOI: 10.48550/arXiv.2107.14082. [Online]. Available: http://arxiv.org/abs/2107.14082.

[4] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," *Frontiers in Computer Science*, vol. 3, Mar. 9, 2021, ISSN: 2624-9898. DOI: 10.3389/fcomp.2021.563060.

[5] K. L. Chiew, K. S. C. Yong, and C. L. Tan, "A survey of phishing attacks: Their types, vectors and technical approaches," *Expert Systems with Applications*, vol. 106, pp. 1–20, Sep. 15, 2018, ISSN: 0957-4174. DOI: 10.1016/j.eswa.2018.03.050.

[6] M. Chawla and S. Chouhan, "A Survey of Phishing Attack Techniques," *International Journal of Computer Applications*, vol. 93, pp. 32–35, May 16, 2014. DOI: 10.5120/16197-5460.

[7] S. Abraham and I. Chengalur-Smith, "An overview of social engineering malware: Trends, tactics, and implications," *Technology in Society*, vol. 32, no. 3, pp. 183–196, Aug. 1, 2010, ISSN: 0160-791X. DOI: 10.1016/j.techsoc.2010.07.001.

[8] T. McIntosh, A. S. M. Kayes, Y.-P. P. Chen, A. Ng, and P. Watters, "Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions," *ACM Computing Surveys*, vol. 54, no. 9, pp. 1–36, Dec. 31, 2022, ISSN: 0360-0300, 1557-7341. DOI: 10.1145/3479393.

[9] K. Lee, S. Sjöberg, and A. Narayanan, "Password policies of most top websites fail to follow best practices," in *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, Boston, MA: USENIX Association, Aug. 2022, pp. 561–580, ISBN: 978-1-939133-30-4. [Online]. Available: https://www.usenix.org/conference/soups2022/presentation/lee.

[10] D. L. Wheeler, "Zxcvbn: Low-Budget password strength estimation," in *25th USENIX Security Symposium (USENIX Security 16)*, Austin, TX: USENIX Association, Aug. 2016, pp. 157–173, ISBN: 978-1-931971-32-4. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/wheeler.

[11] R. A. Maalem Lahcen, B. Caulkins, R. Mohapatra, and M. Kumar, "Review and insight on the behavioral aspects of cybersecurity," *Cybersecurity*, vol. 3, no. 1, p. 10, Apr. 21, 2020, ISSN: 2523-3246. DOI: 10.1186/s42400-020-00050-w.

[12] L. F. Rodrigues, A. Oliveira, and H. Rodrigues, "Main gamification concepts: A systematic mapping study," *Heliyon*, vol. 5, no. 7, e01993, Jul. 18, 2019, ISSN: 24058440. DOI: 10.1016/j.heliyon.2019.e01993.

[13] C. Fischer, C. P. Malycha, and E. Schafmann, "The Influence of Intrinsic Motivation and Synergistic Extrinsic Motivators on Creativity and Innovation," *Frontiers in Psychology*, vol. 10, Feb. 19, 2019, ISSN: 1664-1078. DOI: 10.3389/fpsyg.2019.00137.

[14] A. Bernik, "Gamification Framework for E-Learning Systems in Higher Education," *Tehnički glasnik*, vol. 15, no. 2, pp. 184–190, Jun. 9, 2021, ISSN: 18485588, 18466168. DOI: 10.31803/tg-20201008090615.

[15] F. Marisa, S. S. Syed Ahmad, Z. Yusoh, D. Jatmika, T. Agustina, and W. Purnomowati, "Customer motivation analysis on retail business with octalysis gamification framework," *Journal of Theoretical and Applied Information Technology*, vol. 99, pp. 3264–3279, Jul. 2021.

[16] R. Hunicke, M. Leblanc, and R. Zubek, "Mda: A formal approach to game design and game research," *AAAI Workshop - Technical Report*, vol. 1, Jan. 1, 2004.

[17] A. Mora, D. Riera, C. González, and J. Arnedo-Moreno, "Gamification: A systematic review of design frameworks," *Journal of Computing in Higher Education*, vol. 29, no. 3, pp. 516–548, Dec. 1, 2017, ISSN: 1867-1233. DOI: 10.1007/s12528-017-9150-4.

[18] A. Y.-k. Chou. "The Octalysis Framework for Gamification & Behavioral Design." (), [Online]. Available: https://yukaichou.com/gamification-examples/octalysis-complete-gamification-framework/ (visited on 11/15/2023).

[19] S. A. Andrade Freitas, A. R. Lacerda, P. M. Calado, T. S. Lima, and E. Dias Canedo, "Gamification in education: A methodology to identify student's profile," in *2017 IEEE Frontiers in Education Conference (FIE)*, Indianapolis, IN: IEEE, Oct. 2017, pp. 1–8, ISBN: 978-1-5090-5920-1. DOI: 10.1109/FIE.2017.8190499.

[20] C. Gellner, I. Buchem, and J. Müller, "Application of the Octalysis Framework to Gamification Designs for the Elderly," Sep. 24, 2021. DOI: 10.34190/GBL.21.022.

[21] K. Werbach and D. Hunter, "For the Win How Game Thinking Can Revolutionize Your Business," Jan. 2012.

[22] F. F.-H. Nah, V. R. Telaprolu, S. Rallapalli, and P. R. Venkata, "Gamification of Education Using Computer Games," in *Human Interface and the Management of Information. Information and Interaction for Learning, Culture, Collaboration and Business,*, S. Yamamoto, Ed., ser. Lecture Notes in Computer Science, vol. 8018, Berlin, Heidelberg: Springer, Jul. 2013, pp. 99–107, ISBN: 978-3-642-39226-9. DOI: 10.1007/978-3-642-39226-9_12.

[23] A. M. Toda, A. C. T. Klock, W. Oliveira, *et al.*, "Analysing gamification elements in educational environments using an existing Gamification taxonomy," *Smart Learning Environments*, vol. 6, no. 1, p. 16, Dec. 4, 2019, ISSN: 2196-7091. DOI: 10.1186/s40561-019-0106-1.

Appendix

10.2 Original Project Brief

Enhancing Adults' Understanding of Security Concepts through a Cybersecurity Game

William Mayhew
Supervisor: Dr. Nawfal Fadhel

October 2023

1 Problem

In the modern age, technology saturates many aspects of our lives, but this pervasiveness brings an increase in cyber-attack threats. As a result, individuals need the necessary cybersecurity knowledge to protect themselves. Unfortunately, many people lack the basic fundamentals of these security concepts, leaving them vulnerable to cyberattacks. Consequences can range from personal data breaches to substantial financial losses in businesses. Thus, it is crucial to ensure that the correct measures are taken at all times.

2 Goals

During this project, the primary objective is to teach cybersecurity concepts to a degree which will enhance adults digital safety. I'll use Gamification techniques to develop an interactive tool to make learning enjoyable and effective to ensure engagement. By educating the individuals about cybersecurity issues, they will be able to recognise and address potential vulnerabilities and threats.

3 Scope

This project is mainly targeted towards adults who are susceptible to cyber threats, including working professionals. To enhance the adults' understanding of security concepts, a range of different topics will be covered, starting at a basic level. These topics include, but are not limited to:

- Password security
- Social engineering
- Data protection
- General security practices.

10.3 Project Archive Contents

File	Description
CyberSec Escape Room	Core files of the project
FinalWebGULBuild	Build of the final game for WebGL platforms
Survey Questions.pdf	Survey given to participants

Table 10.1: Project Archive Contents

10.3.1 Contents of CyberSec Escape Room

Within the 'CyberSec Escape Room' folder' the main project files are located within the 'Assets' folder. These include all third party assets used, scripts, objects, and object prefabs. Table 10.2 breaks down the contents within this folder.

Folder	Description
Dialogue	Dialogue scripts in .ink format used throughout the game
Fonts	Fonts used throughout the game
Inputs	Input handlers for the player
Objects	Prefabs and images of game objects
Plugins	Third party plugins utilised (Only zxcvbn)
Scenes	Each scene(stage) of the game
Scripts	All the scripts for different objects/players
ThirdParty	All third party assets from the Unity and Itch.io asset stores

Table 10.2: Assets Contents

10.4 Survey Questions

The questions below are the questions which were asked to participants during user testing. Only one answer was able to be selected at each question, with various opinionated questions being optional.

Pre-Game Questions

1. **What is your age range?**
   a. 18-25
   b. 26-35
   c. 36-45
   d. 46-55
   e. Over 55
2. **How familiar are you with technology?**
   a. Not at all familiar
   b. Moderately familiar
   c. Very familiar
3. **How familiar are you with cybersecurity concepts?**
   a. Not at all familiar
   b. Moderately familiar
   c. Very familiar
4. **Rate your understanding of the following cybersecurity concepts: (Each has a scale of No understanding, Limited understanding, Moderate understanding, Good understanding, Expert understanding)**
   a. Phishing
   b. Romance and Friendship scams
   c. Password security
   d. Cyber policies
   e. Scareware

Participant plays game

Post-Game Questions

5. **How effective do you think the game was at teaching cybersecurity concepts?**
   a. Not effective at all
   b. Slightly effective
   c. Moderately effective
   d. Very effective
   e. Extremely effective
6. **How effective do you think the game was at reinforcing cybersecurity concepts?**
   a. Not effective at all
   b. Slightly effective
   c. Moderately effective
   d. Very effective
   e. Extremely effective
7. **Rate your understanding of the same cybersecurity concepts mentioned earlier: (Each has a scale of No understanding, Limited understanding, Moderate understanding, Good understanding, Expert understanding)**
   a. Phishing
   b. Romance and Friendship scams
   c. Password Security
   d. Cyber Policies
   e. Scareware

Challenge Improvements

8. **What could be improved for the Phishing challenge? (2nd room, accepting/rejecting letters)**
9. **What could be improved for the Romance and Friendship scam challenge? (3rd room, NPC Conversations)**
10. **What could be improved for the Password Workshop challenge? (3.5 room, Creating a strong password)**
11. **What could be improved for the Password Identification challenge? (3.5 room, Identifying strong passwords)**
12. **What could be improved for the Cyber Policies challenge? (4th room, during the boss battle)**
13. **What could be improved for the Scareware challenges? (Throughout game)**

Confidence, Engagement, and Enjoyment

14. **On a scale from 'Learning' to 'Reinforcing', where 'Learning' indicates primarily acquiring new knowledge or skills, and 'Reinforcing' indicates primary strengthening existing knowledge or skills, how would you objectively characterise the game? (Scale from 1-5)**
15. **How confident do you feel in applying the cybersecurity concepts you learned in the game to real-life situations?**
    a. Not confident at all
    b. Slightly confident
    c. Moderately confident
    d. Very confident
    e. Extremely confident
16. **Did you find the game engaging?**
    a. Not engaging at all
    b. Slightly engaging
    c. Moderately engaging
    d. Very engaging
    e. Extremely engaging
17. **What would you rate the overall enjoyment of playing the game?**
    a. Not enjoyable at all
    b. Slightly enjoyable
    c. Moderately enjoyable
    d. Very enjoyable
    e. Extremely enjoyable
18. **Are there any improvements that could be made to the game to enhance overall confidence in applying cybersecurity concepts, increase engagement, or improve enjoyment?**
19. **Was the game responsive? Specifically, was functionality maintained through gameplay without issue**
20. **Did the game stutter at all?**
21. **Was the interface intuitive?**
22. **Was the interface user-friendly?**
23. **Did you encounter any issues running the game?**