**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

# Enhancing Adults' Understanding of Security Concepts through a Cybersecurity Game ...

by William Mayhew

December 11, 2023

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 is to be developed in an attempt to teach those who are susceptible to cyber risks about security concepts and mitigation strategies. The report reviews various cyberattacks and associated crimes to underpin the game's core purpose. Multiple gamification techniques have also been discussed to assist in the development strategy. A plan has been developed for the following phase, outlining the tools, technologies, and intended schedule of the project progression. The hopeful outcome of this project is to teach and enhance the understanding of cybersecurity concepts through an escape room game.

## 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 not used any resources produced by anyone else.**

**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 did not involve human participants, their cells or data, or animals.**

# 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 46% and 32% [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 people's cybersecurity awareness as it 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 accessible to adults across various settings, both professional and personal. However, it's 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 crimes like fraudulent activities and scams such as 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]. One technique used includes spoofing emails to mimic legitimate sources, 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, the email will 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. Its 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 fraudulent methods 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 house deposit into a compromised account, using email addresses closely resembling 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, persuading Zainab to send £6,150 for supposed bills[6].

## 2.3 Discussion

The literature review elucidates the landscape of cyber-attacks, revealing techniques and the subsequent crimes they initiate. 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. Therefore, there is a critical need to strengthen cybersecurity safeguards, particularly in minimising human vulnerabilities.

[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)

# Chapter 3

# Gamification

Gamification involves applying game characteristics in non-game contexts [9]. 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 [10]

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], [11]–[13].

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) so they will be the focus of the following section [14].

## 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) [13]. To describe the aesthetics, Hunicke et al provides a basic list of vocabulary which the game should tend towards [13]:

- 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 [13]. 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 [15]. However, three studies from [12], [16], [17] 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, [12] and [17] identified that Meaning has great motivational influence while [16] showed extremely low influence for Meaning. However, all studies showed that Avoidance was of the lowest influence. This shows the difficulty in optimising 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 [18] developed by Werbach and Hunter, and another developed by Nah et al [19].

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 [18]. 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 [16], [20].

The framework developed by Nah et al defines 5 key principles: Goal orientation, Achievement, Reinforcement, Competition, and Fun orientation [19]. 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 mentioned 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 have. 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 definitely be implemented, and what might not need to 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 her supervisor did not step 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 familiarize 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.

| Story ID | User Story |
|---|---|
| P1-S1 | As Rebecca, I want simulated scenarios involving phishing attacks through emails as well as others 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 customizable 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 recognize 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 customize it to suit my needs. |

Table 4.1: User Stories

## 4.3 Functional Requirements

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

| 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 |
| 6 | Users can access learning material for various cybersecurity topics | Must | P3-S2 |
| 7 | Users can play scenario simulations of attacks | Must | P1-S1, P2-S3, P2-S5 |
| 8 | The game will provide an introduction with instructions for each challenge | Must | P3-S1 |
| 9 | The challenges will have time-limits | Must | P1-S3 |
| 10 | Users can view performance analytics | Should | P1-S2, P2-S2 |
| 11 | The game will provide the user with their strengths and weaknesses | Could | P1-S2, P2-S2 |
| 12 | Users can view a performance leaderboard | Must | P2-S4 |
| 13 | Users can customize the game visually by increasing font size and changing themes | Should | P3-S3 |
| 14 | Users can play against others (multiplayer) | Won't | P2-S4 |
| 15 | Users are rewarded dependent on how well they perform (time, failures) | Must | P1-S3 |
| 16 | Users can customize what content is shown | Could | P2-S1 |

Table 4.2: Functional Requirements

## 4.4 Non-Functional Requirements

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

| 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 be level based to accommodate for further expansion | Must | |
| 10 | The game will store users details securely | Must | |
| 11 | The game will be consistent with accessibility customisations | Should | P3-S1 |
| 12 | The user will strengthen their cybersecurity knowledge | Must | P1-S1, P1-S2, P2-S3, P2-S5, P3-S3 |
| 13 | The game will be relatable to real-life scenarios | Must | P1-S1, P2-S3, P2-S5 |

TABLE 4.3: Non-Functional Requirements

# 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, I have opted for a 2D top-down approach for 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.

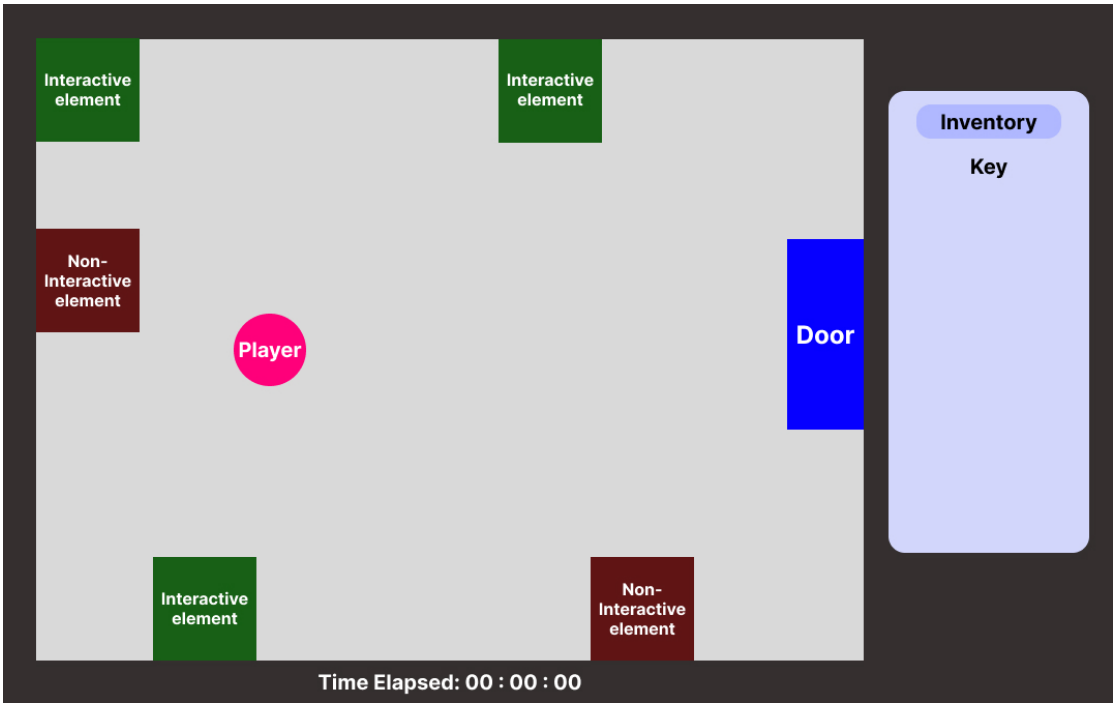


FIGURE 5.1: Wireframe: Game Level

### 5.1.2 Example Challenges

Figure 5.2 is a wireframe of a phishing email detection challenge. This challenge could appear after the player has interacted with an element. 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 is a wireframe of a text messaging challenge. This challenge could appear after the player has interacted with an element. It mimics a text conversation, where the player converses with either a trustworthy or fraudulent user, and has to correctly identify them to pass.

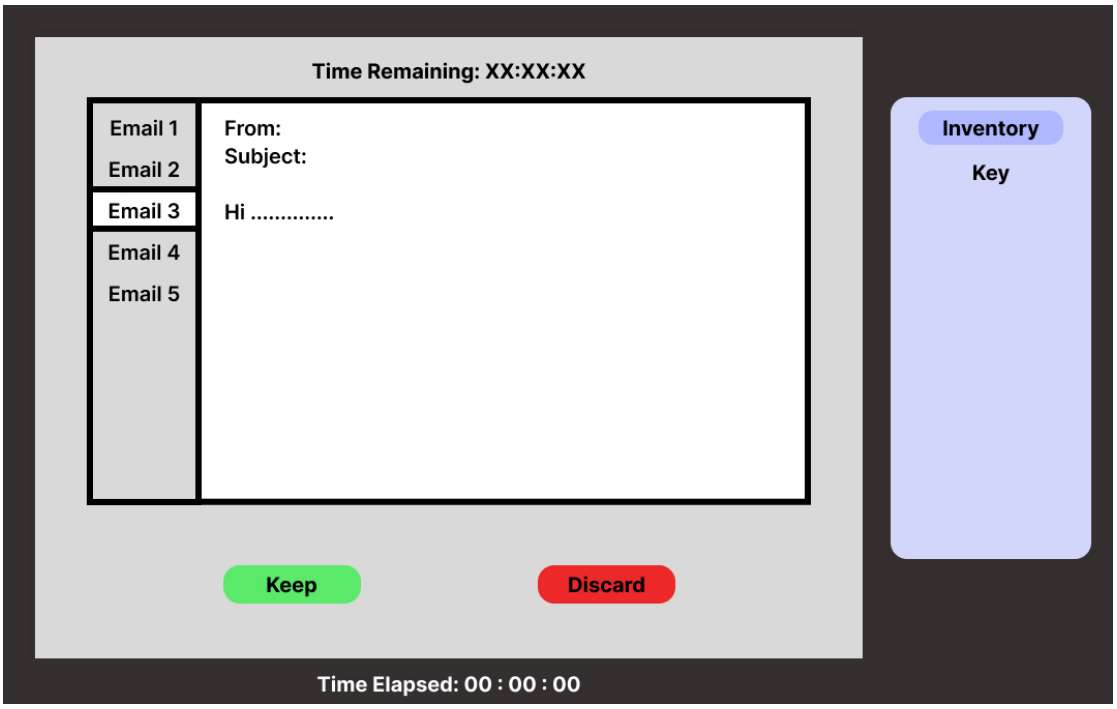


FIGURE 5.2: Wireframe: Phishing Email Challenge

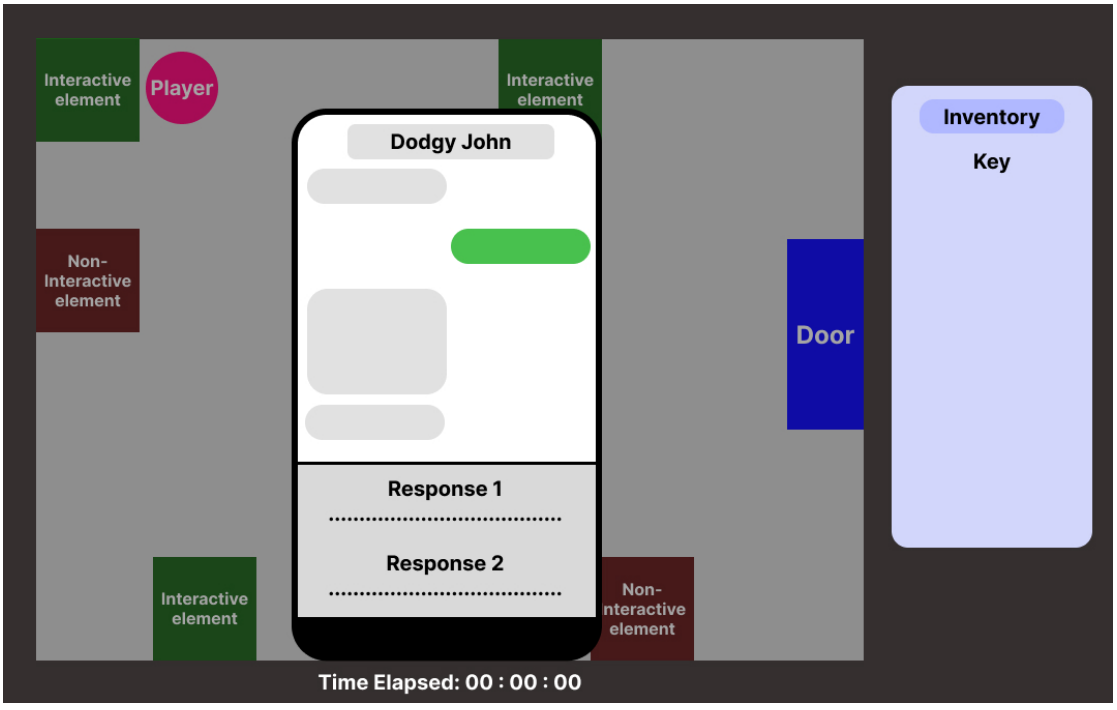


FIGURE 5.3: Wireframe: Text Message Challenge

## 5.2 Activity Diagram

In Figure 5.4, 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, failure prompts further search. Successful challenge completion yields a resource, failure results in life loss. Running out of lives ends the game, while escaping with the key leads to victory.

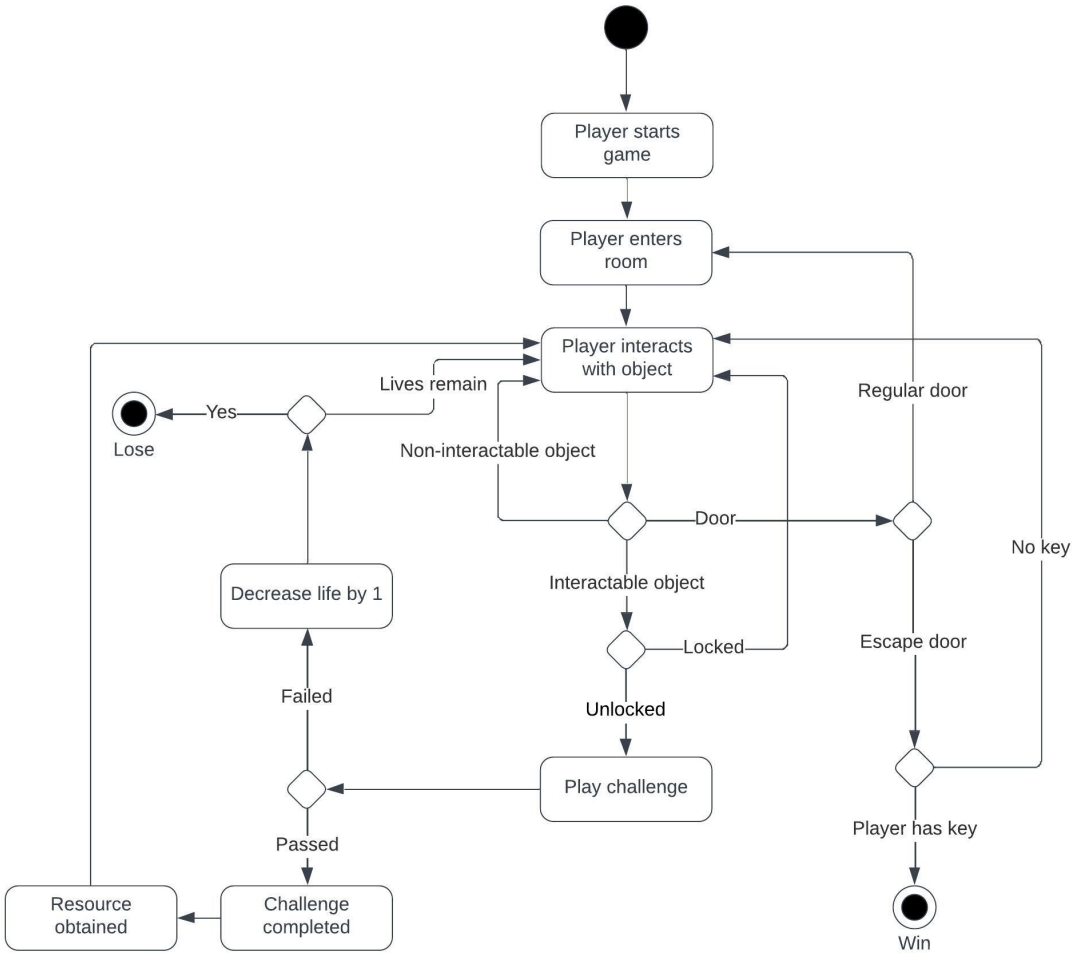


FIGURE 5.4: Activity Diagram: Escape Room

### 5.2.1 Phishing challenge

Below, Figure 5.5 shows an activity diagram illustrating a phishing email identification challenge. This can occur at the "Play challenge" state in Figure 5.4. The

player will be shown a series of emails and they must correctly identify whether they are malicious or safe. Incorrectly identifying an email leads to failing the challenge, which will lead to them losing a life.

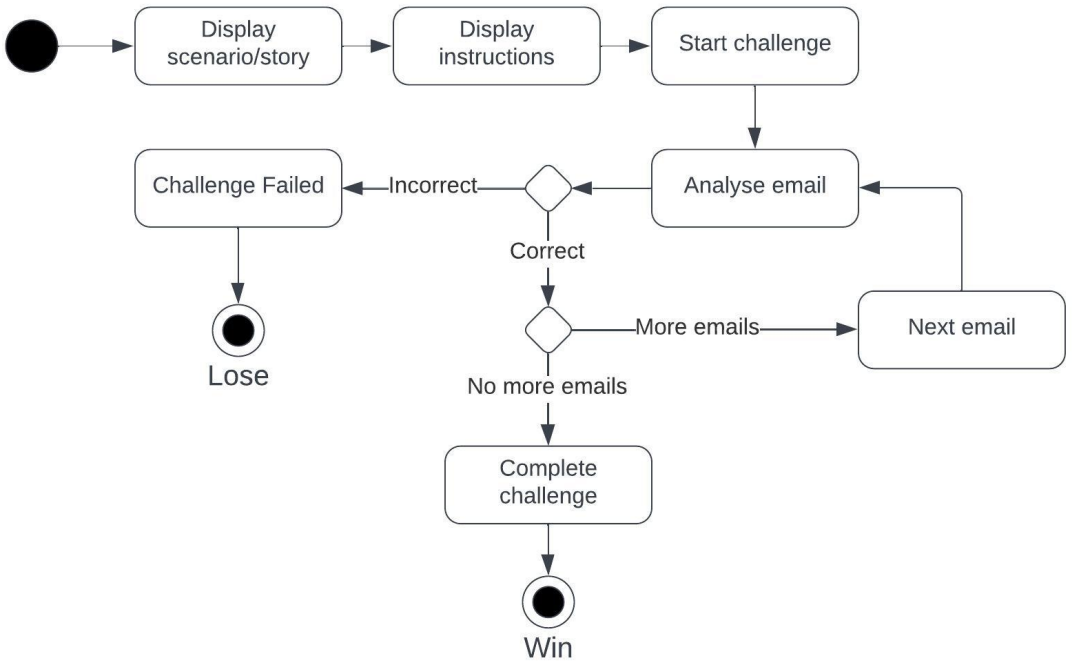


FIGURE 5.5: Activity Diagram: Phishing Email Challenge

### 5.2.2 Text message challenge

Below, Figure 5.6 shows an activity diagram illustrating a text messaging conversation challenge where the player will be required to converse with some recipient. This can occur at the "Play challenge" state in Figure 5.4. The player will partake in a conversation where there are set responses. Their replies must be "safe", not revealing unnecessary information or giving in to the recipient. Replying riskily will result in the player failing the challenge, which will lead to them losing a life.

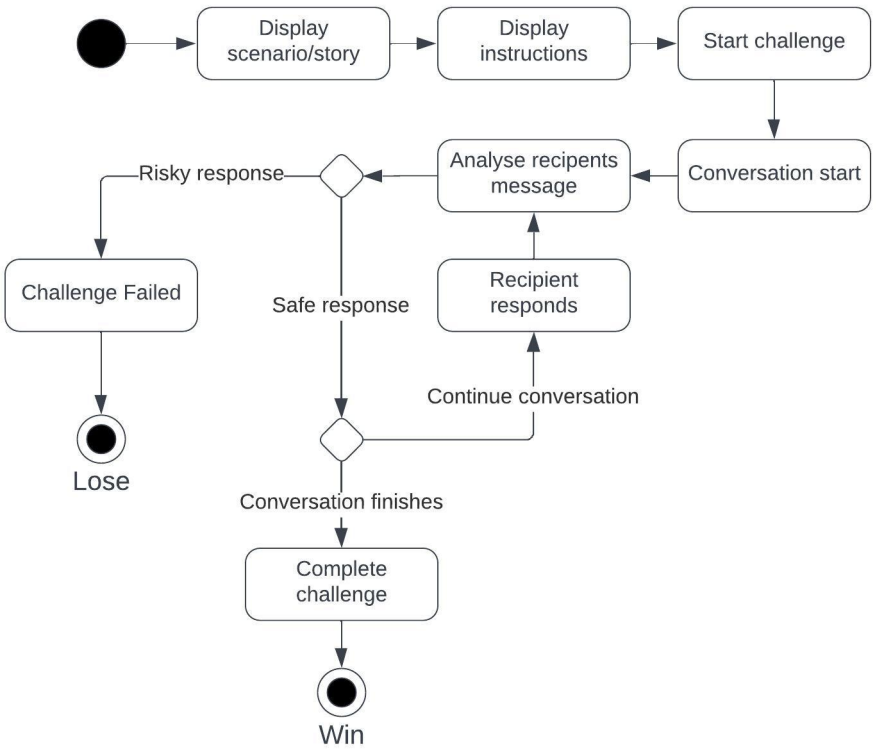


FIGURE 5.6: Activity Diagram: Text Messaging Challenge

## 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 [13].

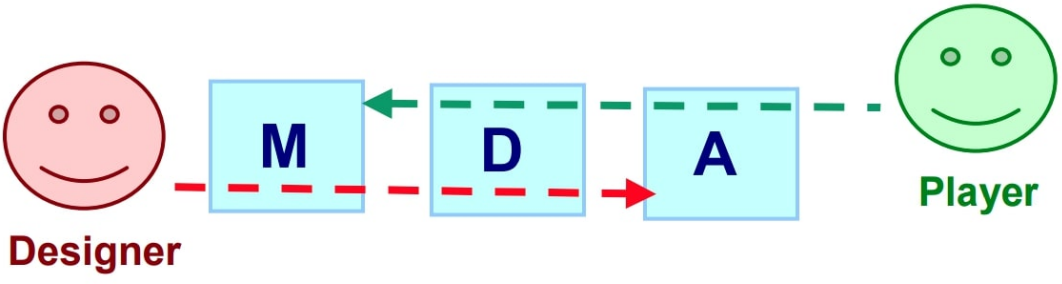


FIGURE 5.7: MDA Framework [13]

### 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 [12], [16], [17]. This can be integrated into the list of words described by Hunicke, where the main aesthetic objectives will focus on **Challenge** and **Discovery**.

### 5.3.2 Dynamics

The dynamics are what create our aesthetic experiences [13]. 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.
- Discovery
    4. Multiple rooms requiring the player to explore and interact.
    5. Resources used to discover hidden or previously locked locations/objects.

### 5.3.3 Mechanics

Mechanics are the fundamental rules and components which will support our gameplay dynamics, affecting the player experience [13].

The mechanics are as follows:

- Navigate room
- Door interaction
- Object interaction

- Challenge timer
- Overall game timer
- Use resource
- Life system
- Challenge initiation
- Keep or discard the email
- Select a text message response
- Complete a challenge
- Collect resource
- Escape room
- Leaderboard of top times

# Chapter 6

# Plan of Remaining Work

The following section will describe the current state of the project, as well as the plan for the subsequent phase. A risk assessment is conducted, and a gantt chart is produced to help schedule tasks and monitor progress.

## 6.1 Development Tools and Technologies

Table 6.1 describes the tools and technologies which have been utilised or are to be utilised in the project.

| Tools | Description |
|---|---|
| GitLab | Project management |
| Lucid Chart | Online software for UML diagrams |
| Zotero | Reference management software for literature research |
| Microsoft Teams | Communication software for meetings |
| C# | Programming language for Unity |
| Unity | Game engine for game development |

Table 6.1: Tools and Technologies

## 6.2 Gantt Chart for Phase 1

| Week | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|
| Date Beginning | 09/10 | 16/10 | 23/10 | 30/10 | 06/11 | 13/11 | 20/11 | 27/11 | 04/12 | 11/12 |
| **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 6.1: Phase 1 Gantt Chart

## 6.3 Risk Assessment

A risk assessment is 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.

The following risks have been identified:

| 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. Utilize online resources and practice |
| Lack of familiarity with Unity development | 4 | 4 | 16 | Allocate learning time for Unity. Utilize 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 |

TABLE 6.2: Risk Assessment

## 6.4 Gantt Chart for Phase 2

Figure 6.2 shows the proposed schedule for phase 2. The application is aimed to be finished on week 26, with weeks 14-17 accounting for the semester 2 exam period.

| Week | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Date Beginning** | 18/12 | 25/12 | 01/01 | 08/01 | 15/01 | 22/01 | 29/01 | 05/02 | 12/02 | 19/02 | 26/02 | 05/03 | 12/03 | 19/03 | 26/03 | 02/04 | 09/04 | 16/04 | 23/04 | 30/04 |
| **Implementation** | | | **Revision/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 6.2: Phase 2 Plan Gantt Chart

# 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 Jan. 2021, ISSN: 2071-1050. DOI: 10.3390/su13042247. [Online]. Available: https://www.mdpi.com/2071-1050/13/4/2247 (visited on 10/29/2023).

[3] A. M. Syed, *Social engineering: Concepts, Techniques and Security Countermeasures*, Jun. 23, 2021. DOI: 10.48550/arXiv.2107.14082. arXiv: 2107.14082 [cs]. [Online]. Available: http://arxiv.org/abs/2107.14082 (visited on 11/13/2023), preprint.

[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, 2021, ISSN: 2624-9898. [Online]. Available: https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060 (visited on 11/11/2023).

[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. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417418302070 (visited on 11/16/2023).

[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. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0160791X10000497 (visited on 12/02/2023).

[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. [Online]. Available: https://dl.acm.org/doi/10.1145/3479393 (visited on 12/02/2023).

[9] L. F. Rodrigues, A. Oliveira, and H. Rodrigues, "Main gamification concepts: A systematic mapping study," *Heliyon*, vol. 5, no. 7, e01993, Jul. 2019, ISSN: 24058440. DOI: 10.1016/j.heliyon.2019.e01993. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S240584401935618X (visited on 11/13/2023).

[10] 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, 2019, ISSN: 1664-1078. [Online]. Available: https://www.frontiersin.org/articles/10.3389/fpsyg.2019.00137 (visited on 11/14/2023).

[11] 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. [Online]. Available: https://hrcak.srce.hr/258425 (visited on 11/14/2023).

[12] F. Marisa, S. S. S. Ahmad, Z. I. Mohd, *et al.*, "CUSTOMER MOTIVATION ANALYSIS ON RETAIL BUSINESS WITH OCTALYSIS GAMIFICATION FRAMEWORK," . *Vol.*, no. 13, 2021.

[13] R. Hunicke, M. LeBlanc, and R. Zubek, "MDA: A Formal Approach to Game Design and Game Research,"

[14] 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. [Online]. Available: https://doi.org/10.1007/s12528-017-9150-4 (visited on 11/16/2023).

[15] A. Y.-k. Chou. "The Octalysis Framework for Gamification & Behavioral Design." (Sep. 5, 2023), [Online]. Available: https://yukaichou.com/gamification-examples/octalysis-complete-gamification-framework/ (visited on 11/15/2023).

[16] 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. [Online]. Available: https://ieeexplore.ieee.org/document/8190499/ (visited on 11/18/2023).

[17] 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.

[18] K. Werbach and D. Hunter, "For the Win How Game Thinking Can Revolutionize Your Business," (visited on 12/10/2023).

[19] 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, Berlin, Heidelberg: Springer, 2013, pp. 99–107, ISBN: 978-3-642-39226-9. DOI: 10.1007/978-3-642-39226-9_12.

[20] 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. [Online]. Available: https://doi.org/10.1186/s40561-019-0106-1 (visited on 12/10/2023).