Department of Computer Science

BSc (Hons) Business Computing

BSc (Hons) Computer Science Digital Media and Gaming

Academic Year 2023 - 2024

Creating Engaging, Timeless Cybersecurity Awareness with a Video Game

Tolu Olasupo

1909933

A report submitted in partial fulfilment of the requirements for the degree of Bachelor of Science

Brunel University London
Department of Computer Science
Uxbridge
Middlesex
UB8 3PH
United Kingdom
T: +44 1895 203397
F: +44 (0) 1895 251686

Abstract

Cyber security remains to be an ever-pressing issue in society. The digital landscape is always expanding with new technology, new apps, new users, new platforms and so much more. Despite all the advancements being made in cyber security, the threat landscape expands just as rapidly. Even as cyber security experts work tirelessly to create safety measurements, human error persists as the leading cause of most data breaches and cyber-attacks across personal and business domains.

In my attempt to address this problem, I decided to create an educational game in Unity 2D that would teach players about cyber security; primarily how to recognise, deal with and avoid cyber threats and malicious actors. The main gameplay loop consists of the player answering emails, trying to decipher the intent of the sender, and choosing a correct response. These emails can also require the user to do certain tasks related to cyber threats and methods of attacks, focusing on attacks that are the most challenging for people, such as phishing. This game also has a progressing story that highlights some behaviours that can invite or prevent cyber-attacks.
My contribution to solving this issue was a learning experience that can teach the fundamentals of handling and mitigating cyber threats, which can be relevant to most threats. This method prioritises scenario-based teaching over information recital. This experience has been designed to be memorable, so players retain the knowledge they gained long-term, and act as training that appeals to both the public, and employees under-going professional training. It proved to have potential to appeal to both groups.

Acknowledgements

I thank all the teachers and lecturers that have taught me from childhood to present day. All of them fuelled my imagination and creativity and equipped me with the knowledge that I needed to complete this dissertation.

I thank my supervisor, Jeff Wen for helping me through the entire process of undergoing this project. His guidance made understanding things much easier, and I would not have been able to navigate this extensive task without him.

I would also like to thank my dad, mum, and sisters for supporting me and my dreams and aspirations. Without them, I wouldn't be as confident in pursuing the route I decided to choose. Their prayers for me have been answered and I will continue to make them proud.

And finally, I thank the God for seeing me through all the challenges that life threw at me before getting to this point. Every day I live and every breath I take is a blessing from you, and I pray that I continue to put all my trust in you for the rest of my life. Jesus is Lord.

I certify that the work presented in the dissertation is my own unless referenced.

Signature Tolu Olasupo

Date 22/03/2024

Total Words: 15353

Table of Contents

List of Tables

List of Figures

1 Introduction

In today's world, technology has relevance in all aspects of life. Even professions far removed from IT will prove to benefit from technology somehow; whether it be leveraging the power of automated tasks or using social media to network and promote business. This has resulted in an endless stream of new users using the continuously expanding library of information and platforms that the internet is, regardless of their background or career path. Despite this, there is a shadow that expands at a similar rate, and grows to be just as complex, this being cyber threats.

Cybersecurity is the practice of protecting computer systems, networks, and data from digital attacks, unauthorized access, or theft. It is comprised of various processes and practices to maintain the safety of private information and domains. Cyber threats have been a constant companion to technology's evolution; malicious actors use the same innovative systems and technological developments that we do. We can observe this truth through recent events, such as the rise of generative AI resulting in attackers creating more deceptive phishing emails and create more sophisticated social engineering content (Check Point Research 2023). Despite years of effort to empower digital defences, threats always find new methods of attack. When we consider the combination of an infinitely evolving threat landscape, and the endless stream of new users with varying experience with technology, the scale of the challenge is clear.

Education and training are crucial in cybersecurity, serving as the primary defence line. They equip individuals with knowledge to recognise threats and prevent common mistakes that enable data breaches, both personally and professionally. However, despite various awareness efforts, human error remains the root of most data breaches (Fortinet 2023). It's expected that users, being the primary access point to systems and private data, inadvertently cause breaches, yet it's concerning when leaders observe that even trained employees fall short in cybersecurity awareness (Fortinet 2023). Given human error's significant role in cracking defences and leaders doubting their train employees' knowledge, it prompts the question: Is current cybersecurity awareness sufficient?

This question led me to doing research on various campaigns and training programs around cybersecurity with a critical eye. Upon doing research, I came to a few realisations:

1. There is a strong focus on being informative.

Both campaigns and training typically present information differently: campaigns use concise content for broad appeal, while training offers in-depth knowledge. However, both lack emphasis on practical experience, often resorting to quizzes or tests that merely encourage information recital, rather than providing real practice. This observation led to my next realisation:

2. Cybersecurity is difficult to “practice”.

Practice is crucial for learning, it enables students to directly understand the consequences of their actions, like how driving lessons emphasize the importance of traffic laws for example. However, cybersecurity education faces challenges with mimicking this practice method, as hacking a person real data for the sake of teaching is neither safe nor ethical. This limitation highlights why current awareness methods may not effectively change behaviour; information alone, without practical experience, lacks relevance. Recognizing this, I advocate for integrating informative content with practical experiences, guiding my proposal for a more effective learning approach in cybersecurity.

My solution is an educational game that teaches cybersecurity through interactive play and mechanics inspired by real scenarios. This approach aims to transform learning into an engaging and memorable journey, where players navigate a story infused with cybersecurity themes, making education both informative and entertaining.

1.1 Aims and Objectives

The over-arching aim of my project is:

"To enhance cyber security awareness among the general public through an interactive game that integrates real-world cyber threats and scenarios, to encourage long-term retention and proactive digital safety practices."

By creating this game, cybersecurity education would have more appeal to even those not undertaking training, since the game would also act as entertainment with its story and gameplay. But for players that have undertaken training, the game experience acts as a method of training, and attributing accumulated cybersecurity knowledge to a fun experience. So regardless of a player's background, there is a benefit to playing the game.

To reach this aim, I have a few objectives:

1. Incorporate several cyber security concepts that cover most common cyber-attacks within gameplay, to cover the most vital cybersecurity information.

2. Design and implement unique game mechanics for the different cyber threats and common errors that lead to breaches, to make each threat stand out.

3. Represent threats to a user's cybersecurity both inside and outside of the digital landscape to encourage a change of cybersecurity habits rather than only threat recognition.

4. Create mechanics that can act as a form of cybersecurity "training" for both experienced and un-experienced players.

5. Create an engaging learning experience by creating an interesting story/narrative that ties into the topic of cybersecurity.

1.2 Project Approach

I will approach this cybersecurity educational game project using methods akin to those used by game developers. Initially, I'll conduct thorough research on cyber threats, human error, and existing awareness efforts to determine the game's requirements and objectives. This research will shape the game's concept, including its storyline, genre, gameplay mechanics, and how these elements will engage players in cybersecurity learning.

The design phase will map out the game's structure and system interactions within C#/Unity, utilizing pseudocode and diagrams to outline object interactions. Using C# and Unity, I will develop the game, focusing on integrating and testing features simultaneously. To evaluate the game's impact on enhancing cybersecurity awareness, playtesting with pre- and post-gameplay surveys will gauge players' knowledge improvements, attitude shifts, and overall engagement with the game.

1.3 Dissertation Outline

Chapter 2: A discussion on the background of my project, what solutions exist to the identified problem, how they attempted to solve the problem, and their strengths and weaknesses.
Chapter 3: A look into the methodology utilised for this project.
Chapter 4: Designing the educational game and its mechanics and features.
Chapter 5: Implementing the games features in Unity and programming in C#.
Chapter 6: Testing the functionality of various aspects of the game.
Chapter 7: The evaluation of the pre- and post- gameplay survey results.
Chapter 8: An evaluation of the project against the objectives.

2 Background

2.1 Cybersecurity Challenges

The background review's origin stems from a general look into the current landscape of cybersecurity, including common issues and the role of human error in the field. The first background source I reviewed was a very recent look into the state of cybersecurity at the time, focused on the human element of cybersecurity.

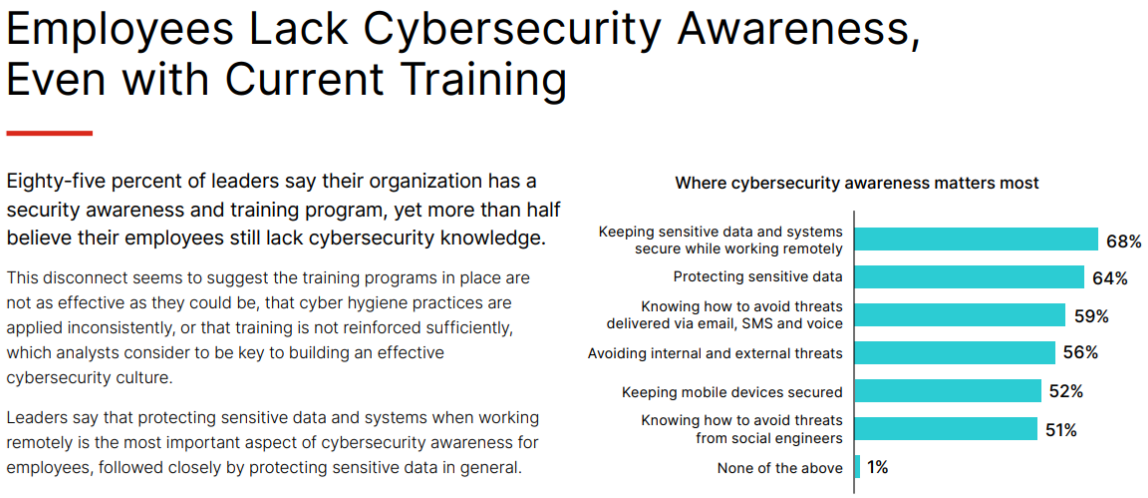

Figure 1 - Page 9 of "Fortinet 2023 Security Awareness and Training Global Research Brief" (Fortinet, 2023)

This brief investigates cybersecurity at the organizational level. By a large margin, attackers are focusing their efforts on users, primarily with phishing, malware, and password attacks. These attacks target poor habits (or cyber hygiene). The most important portion of this brief, for my project, is the concern of a lack of awareness despite training being in place for 85% of organisations (Fortinet, 2023). This almost directly places current training programs under scrutiny, specifically regarding their ability to reinforce learning.

It may be easy to claim that the ever-evolving cyber threats make training obsolete. While threats do evolve, it is not only new kinds of attack methods that malicious actors use. Report by *Checkpoint* (Horowitz, 2023) highlights how both new and old methods of attacks are prevalent in modern day. This includes the usage of USB drives that carry malicious payloads, on top of the usage of generative AI making sophisticated social engineering content (Horowitz 2023). But even newer methods of attack are mostly just more sophisticated versions of older methods, so training can realistically cover any new method without having to tailor to specific new developments such as ChatGPT. However, it is also possible that training fails to teach cybersecurity at a fundamental level; a level that would apply to any new developments with cyber-attacks.

Failure to teach and spread awareness about cybersecurity does not only apply to training programs, but campaigns too. This is more common, as training can at least condition students to care about a topic for the period of the course; campaigns have the included burden of building interest in a topic for people to pay attention to them. However, perhaps the lack of interest building in training could be negatively affecting knowledge retention?

"Effective influencing requires more than simply informing people about what they should and should not do: they need, first of all, to accept that the information is relevant, secondly, understand how they ought to respond, and thirdly, be willing to do this in the face of many other demands" (Bada, Sasse and Nurse, 2019). Informing is important, but without influence it is less effective. Influence assigns value to information on a subconscious level, using persuasion techniques such as fear, humour, expertise, repetition, intensity, and more to create a long-lasting impact on people (Bada, Sasse and Nurse, 2019).

2.2 Traditional Cybersecurity Education and Awareness

Cybersecurity campaigns are the most far-reaching tool for cybersecurity awareness, used to create a culture that is proactive about cybersecurity, creating good habits that keep users and systems safe. They utilize short-form content such as posters, flyers, and social media posts (NHS England, 2023), along with interactive webinars, videos, infographics, workshops, and online quizzes. These resources often feature easily digestible tips on password security (Kate, 2023), recognizing phishing attempts, updating software (Puzder, 2022), and safe browsing practices. One of the biggest campaigns is "Cybersecurity Awareness Month", a campaign that started in the US in 2004, and eventually became adopted worldwide as a month every October to encourage proper cyber hygiene and habits (National Cybersecurity Alliance, 2022).

These campaigns excel at simplifying information, exposing bad habits, and suggesting easily actionable preventative measures. However, a common issue with these is a lack of practical understanding and engagement (Smith, D.T. and Ali, A.I., 2019). While people can understand the information given to them, there is no immediate incentive to use or remember said information. The lack of influence, or use of persuasion techniques, results in information falling on deaf ears (Bada, Sasse and Nurse, 2019). However, improvements can be seen when influence is introduced. Smith, D.T. and Ali, A.I., (2019) for example saw great effect when disguising a cybersecurity lesson as a game programming lesson; this approach introduced an element of surprise, proving how the cybersecurity information was relevant to them before even giving them the information.

Online courses and training have more of a luxury in terms of having the participants attention. Participants take courses for the purpose of learning, often for a reward like a certification. As a result, these courses can dive deeper into the details about aspects of cybersecurity, using videos from industry experts, quizzes, articles and more. Websites such as IBM and Codeacademy offer well received courses on cybersecurity for beginners and experts. Courses are very informative, and encourage knowledge retention through tests, quizzes, and incentive through certification. However, they can face the issue of long-term knowledge retention. It is dependent on what the student's intentions are: learning for the knowledge or learning for the certification. The latter can result in cramming knowledge to pass the tests, which negatively effects knowledge retention (Lindsey, Shroyer, Pashler and Mozer 2014).

2.3 Gamification in Education

The potential of education games has long been realised. They have been recognised for their ability to create an engaging learning experience; they are very prevalent in children's education for that reason. Generally, they aim to "balance the subject matter with the game play and the ability of the player to retain and apply said subject matter to the real world." (Peña-Miguel and Sedano Hoyuelos 2014). Educational games can stimulate learning motivation, improve learning outcomes, create engaging learning environments, and promote innovative learning methods. (Zeng, J., Parks, S., and Shang, J. 2020)

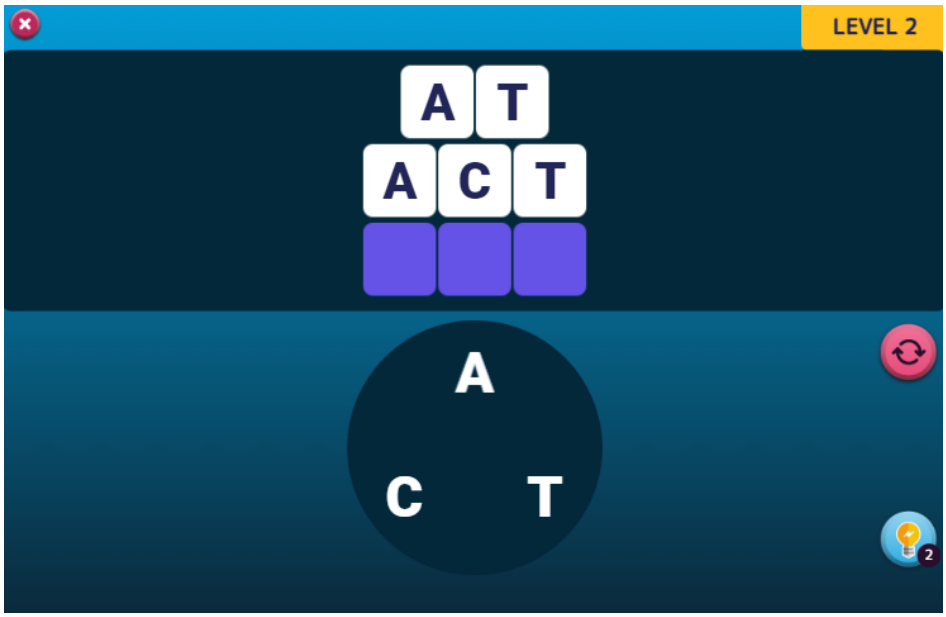

Figure 2 – Screenshot of "Wordgame" by ImproveMemory (https://www.improvememory.org/brain-games/word-games/word-game/)

The most common form of educational game is the puzzle game, where players are required to complete unfinished pieces of information, often using unordered details or clues. For example, a simple word game as displayed in figure 2, where players must use letters to create as many

words as possible. These games are easy to create; conceptually they are created by taking a complete piece of information, extracting key words or details from the information, and getting players to use their own knowledge to put the information back together. This type of educational game is very simple in concept, as they act very similarly to tests and examinations, where students are expected to do the same.

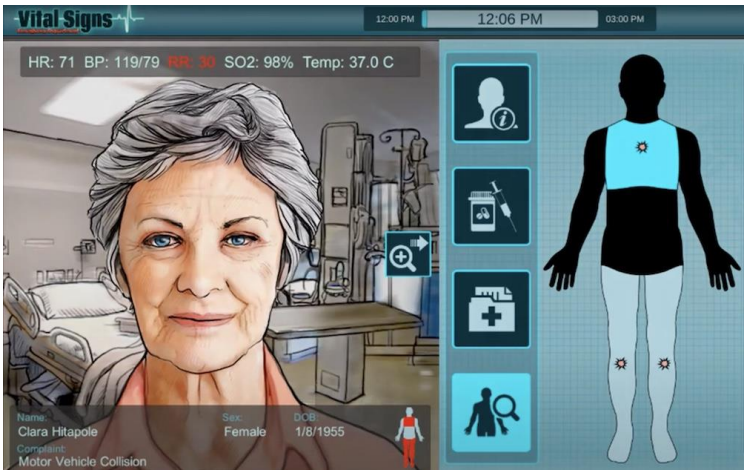

Figure 3 - Screenshot of "Vital Signs: ED" by BreakawayGames (https://www.healthysimulation.com/serious-games/)

At a higher level of education, educational games (called serious games), focus more on their ability to simulate real life scenarios, and act as a risk-free environment for practical experience. (Backlund and Hendrix 2013). One example is figure 3, a game based around an emergency department that simulates taking care of patients in a high stress environment. These kinds of games are considered genuine training material, and have shown to improve the performance of professionals, such as surgeons, in real world situations (Backlund and Hendrix 2013). This gives players the incentive to return to these games; to refresh their knowledge and improve at a skill. The mechanics of these games are directly inspired by their real-life counterpart, unlike the various educational puzzle games that simply adopt the puzzle format.

Looking into educational games, we can see two dominant groups: puzzle games and simulation games. They are designed for different audiences and for different reasons. Puzzle games are good at making education engaging, especially for younger audiences. However, there is a lack of support for sophisticated game mechanics found in commercial video games, and a limitation on the variety of interactive activities they can offer (Antonova, Bontchev 2019). Simulation games offer unique mechanics inspired by their real-world concept and can act as training due to their accuracy. However, the target for these games are often professionals or students already within the field of whatever concept the simulation is teaching. These two types of games parallel the difference between awareness campaigns and training. Campaigns and

puzzles are for easier, short-form information and learning, but are limited in their ability to influence the reader/player into believing their information is valuable. Training/courses and simulation games are more immersive and detailed, aiming to deepen understanding and skills through realistic scenarios. However, they are heavily dependent on the student/player's intentions, whether it be for a genuine deepened understanding or to simply receive a certification. Creating engagement or interest is generally second to informing people and training their skills when it comes to both training courses and simulations.

2.4 Educational Cybersecurity Game Solutions

Educational cybersecurity games are no new concept and have shown positive results to learning in the past, across different genres of game (Alotaibi, Furnell, Stengel, and Papadaki 2016). Most of these games adopt the puzzle format, as is expected with the reasons given in the previous section (Hendrix, Al-Sherbaz, Victoria 2016).

Figure 4 - Screenshot of "Cyber City" by CybergamesUK (https://cybergamesuk.com/)

However, there is some more variation with cybersecurity educational games, as the topic of cybersecurity has proven to be more of a requirement for older audiences than younger ones (Branley-Bell, Coventry, Dixon, Joinson, Briggs 2022). One of these examples is *Cyber City* by *cybergamesuk*, an educational game comprised of various minigames related to cybersecurity concepts such as phishing, protecting networks, firewalls and more. This game, and similar cybersecurity games, attempt to make learning engaging by creating scenarios around these cybersecurity concepts.

Figure 5– Screenshot of "Cyber City", Rogue Wifi Minigame by CybergamesUK (https://cybergamesuk.com/)

These games do add context to information, *Cyber City* makes different cyber threats and concerns feel unique by having different games for each. Although, the quality of these cybersecurity games varies greatly. The best of these games are the ones that use cybersecurity concepts to influence mechanics, like the Wi-Fi minigame (Figure 5), where the player must choose the correct Wi-Fi signal in the café and enter the password.

Despite how these games attempt to engage players, one cannot help but notice the large disconnect between serious games, and entertainment games that reach mainstream. "It could be argued that serious games fail to reach large audiences and that their potential is only exploited in formal contexts. Indeed, only people aware and convinced of the benefits of serious games will promote and implement serious games in their organization or business." (Le Compte, Elizondo and Watson 2015). Ultimately, very few of these serious games reach a large audience for a few reasons.

- They are not distributed in a similar manner to commercial games sold in games stores or online game stores.
- They have no incentive or value outside of formal settings.
- They have no replay value.
-

We can look at an example of a popular game with other benefits, such as *Wii Fit*, a Japanese fitness game created by *Nintendo*. Despite being used widely for fitness, it has seen extensive use outside of formal settings due to its visibility on one of the biggest consoles of all time, as well as an extensive number of mechanics, features and more that are not purely for fitness (Nitz, Kuys, Isles, Fu 2010). If educational games are to spread awareness, they must remember their identity as games, and appeal to those that are not specifically seeking to learn.

We can even look at serious games that were not published by a previously established company. *Undertale* was a role-playing game published in 2015 by an independent developer, Toby Fox. This game resonated with millions of people around the world for its storytelling and unique spin on RPGs, it remains a talking point in pop culture almost a decade later. This game uses story and gameplay to encourage players to think about their actions and consider non-violent alternatives to conflict. It was able to bridge the gap between serious games and entertainment game by weaving its lessons on morality into gameplay mechanics and story. Meanwhile it equally focused on creating a memorable experience with those same elements, combined with music, characters and dialogue that evoked emotional reactions (Müller 2017). Games like Undertale are the golden example of what a game should be if it intends to spread awareness or a message: a healthy balance of a genuine piece of entertainment, and educational elements that are vital to the experience.

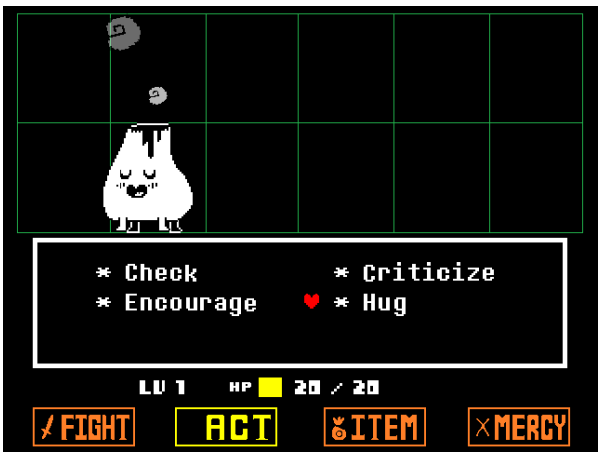

Figure 6 - Screenshot of "Undertale" in game, Example of the alternative actions players can take to "defeat" an enemy. (Taken from https://undertale.com/about/)

From my research, I have identified common cybersecurity challenges; solutions for spreading awareness and their effectiveness, the power and novelty of education games, and existing cybersecurity games and the effectiveness of them. This research has highlighted to me that incentive is a very important factor regarding knowledge retention and building interest. To properly influence a person, it requires some sort of emotional response, or an acknowledgement that the information provided to them is worth remembering. To reach a wide audience, it is important that a poster, article, video, or game can appeal to a person before feeding them information. The superior education game solutions are ones that can find the balance between education and entertainment; making use of their educational elements to influence the game experience in a way that does not disturb it.

3 Methodology

This project aims to address the critical need for improved cybersecurity awareness amongst the public, using an educational game as a method to grow interest in the topic and support longer knowledge retention. The project is guided by a few research questions:

1. What are the current common threats and errors that people face when it comes to cybersecurity, and how can they to be dealt with?
2. How can I make a learning experience appeal to a person, regardless of experience/knowledge?
3. How can I design a learning experience to be memorable, and make the information easier to retain?

My project used the agile development methodology. This methodology is very commonly used within game development due to its flexible nature, and emphasis on consistent testing and integration. This methodology is also well suited for smaller teams, such as me, due to its flexibility. Given the time I had to complete this project, the agile methodology would give me the opportunity in later stages of development to re-assess what is possible in the given time.

Research includes further research into cybersecurity to find which concepts I want to prioritize teaching to players over others. In extension, this will support the process of defining the story, gameplay loop, setting, and overall direction of the game. For the most part, this will be about finding the common threats and errors that people face regarding cybersecurity and how they operate.

Design focuses on conceptualising the game's structure, content, and mechanics, using the research from the previous step as inspiration for how these different aspects will work. This phase will be part of the iteration loop and will be revisited upon adding each mechanic. The first design iteration will be focused on the skeleton of the game such as main story, basic controls, and other foundational aspects. Later iterations will focus on specific mechanics.

Implementation and Testing includes development using Unity, chosen for its flexibility and wide support for creating games, also due to my very recent experience using the tool. The programming language likewise will be C#, the main language used for Unity. Features will be tested as they are implemented. Unit testing will be the main tool for ensuring functionality.

The **evaluation** focuses on assessing the educational impact of the game on players' cybersecurity awareness and behaviours. This will involve conducting pre- and post-gameplay surveys with a group of testers to measure any improvements in knowledge, and to gain a consensus on if the game is truly both engaging and educational. A link to the game download and the surveys will be sent over to testers so that they are able to test the game in their own

time. This method is more time efficient compared to interviews and any other form of in-person assessments/testing and allows complete flexibility for the testers.

I believe this to be the best approach for this sort of project, given both the context and the timeframe that this project. The agile methodology allows a great level of flexibility for the project. Pre- and post-game surveys allows me to measure any change in cybersecurity knowledge and habits, while also measuring engagement and interest the game has generated.

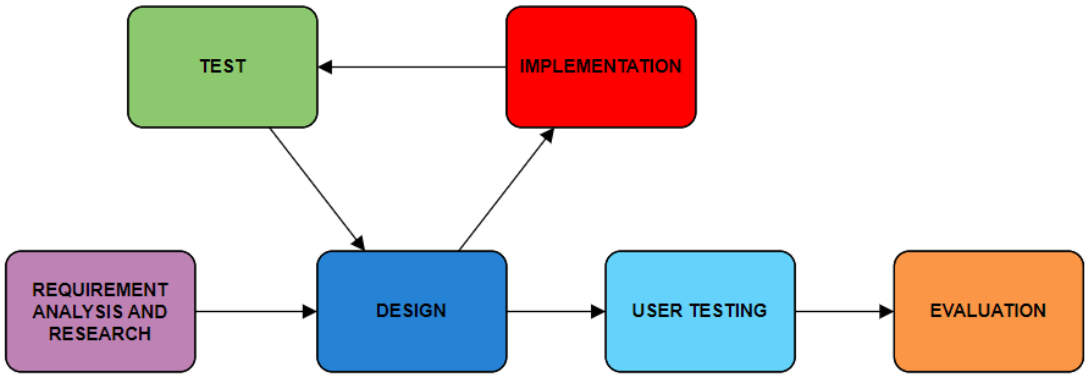

Figure 7 – Agile Methodology Diagram

4 Game Design

4.1 Research – Gathering Requirements

I first defined what cybersecurity concepts I would need to teach and explain. These concepts were to serve as the educational backbone of the game, influencing the story and gameplay.

Threat/Error	Description
Malware	Any software intentionally designed to cause damage to a computer, server, network, or device. Examples include viruses, worms, trojans, ransomware, and spyware.
Phishing	Attackers impersonate legitimate entities, such as companies, organizations, or individuals, to trick users into revealing sensitive information. Often involve deceptive emails, text messages, or websites that appear to be legitimate but are designed to steal information.
Spoofing	Impersonating another entity or source to deceive users or gain unauthorized access to systems or data. This can include IP address spoofing, email spoofing, caller ID spoofing, or website spoofing. Can be used in conjunction with other types of cyber-attacks, such as phishing or man-in-the-middle attacks.
Brute Force Attack/Weak Passwords	Trying all possible combinations of passwords or encryption keys until the correct one is found. Often used to gain unauthorized access to user accounts, systems, or encrypted data. Simple passwords are the easiest the break.
Insider Threats	When individuals within an organization misuse their access privileges to harm the organization's systems, data, or operations intentionally or unintentionally. Can include employees, contractors, or partners who abuse their privileges, steal sensitive information, or sabotage systems.
Man-in-the-Middle	When a malicious actor intercepts and alters communication between two parties without their knowledge or consent. Can occur in various communication channels, including Wi-Fi networks, email, and web browsing.
Social Engineering	Manipulate individuals into divulging confidential information, providing access to systems, or performing actions that compromise security. This can involve techniques such as pretexting, phishing, baiting, or tailgating.

Table 1 - Common Cybersecurity Threats

In Table 1, we can see some of the threats that were highlighted throughout my research. All of them are threats that target a user in some way, through networks, other people, emails and more. There is a notable amount of overlap between these threats, such as phishing or spoofing being used to trick users into downloading malware.

4.2 Story – Adding Context and Structure

To be able to weave these concepts into a game, I needed to create an over-arching story that would allow these concepts to flow into the game loop seamlessly. The story will play a critical role in engaging players, building interest in more than just the learning experience. Welsh, E.M. (2017) outlines the proper structure for creating a story so I followed their format.

Story Outline

"A man has found a job as an office worker. However, the company 'Corpo', that hired them is secretly a hostile work environment, where many employees try to rise to the top by bringing other employees down; aiming to get fellow employees fired by any means. Corpo has become very unstable and is guaranteed to collapse on itself if nothing changes. However, jobs are very difficult to find so our new hire must survive in this workplace until it either changes its ways or falls through. "

This story itself is designed to be a cautionary tale to people and corporations. It allows the player to see and experience poor behaviours and environments that can encourage cyber attacks and data breaches. Players will be able to sympathise with the main character due to their dilemma of needing a job and staying in a poor workplace, creating more investment.

Genre (Type of Game)

This is a single player, role-playing game (RPG), a game where a player assumes the role of a character in a fictional setting. Players follow the story and gameplay through the perspective of the player character. The game runs in Unity 2D, and will therefore be a 2D RPG, I chose a pixilated style for simplicity.

Figure 8 – Screenshot of "Pokemon Diamond and Pearl" by The Pokemon Company, Example of the visual style I saw my game looking like. (Taken from https://tcrf.net/Proto:Pok%C3%A9mon_Diamond_and_Pearl/English_Kiosk_Demo)

The World and Characters

The game is set in the modern age, inside of a singular town. Gameplay will mostly take place inside of an office in this town, where the player will work each day for the company. The main characters will consist of the following:

Character	Role	Description
Steve	Player Character/Protagonist	• Main character of the story. • New hire at the company. • Quiet character that doesn't speak much.
Mark	Main Antagonist NPC (Non-Player Character)	• Main antagonist of the story. • Manager of the company 'Corpo'. • Lazy, likes quick, cheap, and easy results, main reason why the workplace is toxic.
Fred	Supportive Character NPC (Non-Player Character)	• Non-hostile employee. • Line Manager of "Steve", the main character. • Trustworthy character. • Gives the player tips and instructions on completing certain tasks.
Q	Supportive Character NPC (Non-Player Character)	• Suspicious character with unknown motives. • Knows a lot about the toxic environment of 'Corpo'. • Stands outside of the 'Corpo' building to give the player advice on specific threats they will encounter each day.

Table 2 - Main Characters and their Roles

There will also be a multitude of name-less NPCs that will exist in the town and the company building. Some of them will be normal, but others will be active threats to the player, and players will have to decipher who has normal intentions and who has bad intentions.

These are the areas that were initially planned for the game:

Area	Description
Town	The area where the game takes place. In-game, the player will walk through town to get to work at the start of each day. The town will have various NPCs that the player can talk to. The player will also be able to talk to *Q,* for information on what may occur on each day at work.
Meeting Room	The room where Steve will meet with his team at the start of each day. The player will see a conversation about what their tasks are each day and will be able to see the atmosphere of the team become more hostile each day, bringing new challenges.
Main Office	The main area for gameplay. The player gets their tasks done here each day for work. There will also be other workers (NPCs) inside the office during the day in their own areas. The player will have their own PC and cubicle.
Manager Office	The office that the player will be called to at the end of each day. Their manager will go over the players performance each day, whether they properly completed the level or not.

Table 3 - Main Game Areas

Story Structure

The main story is linear, it progresses day by day for about the span of a week. Each day, there is a new challenge for the player, and every day the workplace becomes more hostile. By the end of the week, there is an event that causes a large portion of the company to resign, leaving the player to complete a very challenging final day where they are forced to handle all of the team's work. After this day, the player character, Steve, will also leave the company due to the stress and bad practices. The story ends with the manager, Mark, being fired by the regional manager, and the company, Corpo, finally changes their ways and improves their practices and fosters a better work environment.

Not all story elements had been decided at this stage, as the mechanics I would eventually add would impact on the story too.

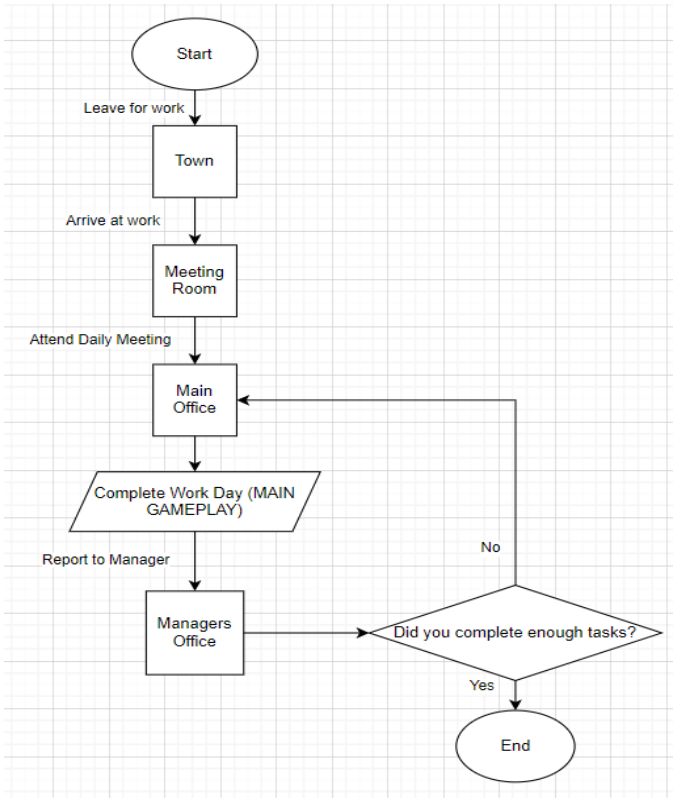

Figure 9 – Flowchart of the game loop for any given day/level.

4.3 Gameplay Loop

My idea for the gameplay was that each day, the player would have a set amount of time to complete a set number of tasks.

- The player wins when they complete all tasks in the time limit.
- The player loses if they do not complete all tasks in time, or if they fail too many tasks.

Tasks would be related to the cyber threats/errors already highlighted during research.

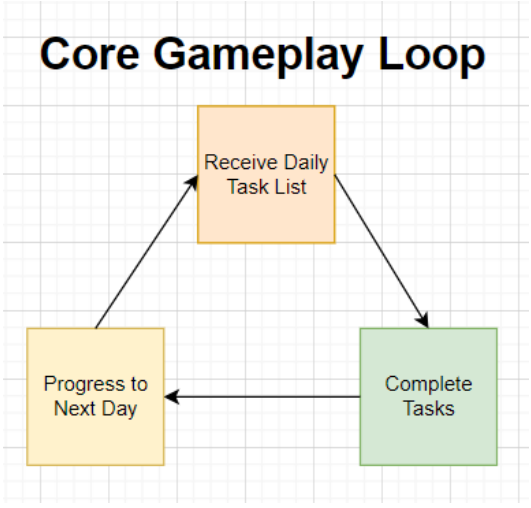

Figure 10 –Challenge > Action > Reward formula. (Brazie 2024).

The loop in figure 3 describes the flow for each level.

1. The player receives their tasks for the day, this also includes conversations with characters prior to the timer starting.
2. The player must complete all tasks given to them.
3. The player completes their tasks and can progress to the next day.

4.4 Level/Area Design

Highlighting the important areas of the game gave me the opportunity to begin designing them. I used the software called "tiled", an open-source software for game-developers used to create 2D maps for games. I used open-source tile sets (a collection of images) to create each map (tile sets and all other assets that I used will be credited to their respective owner in another file). On top of designing maps, this software has the benefit of being able to import maps directly into Unity.

Main Office

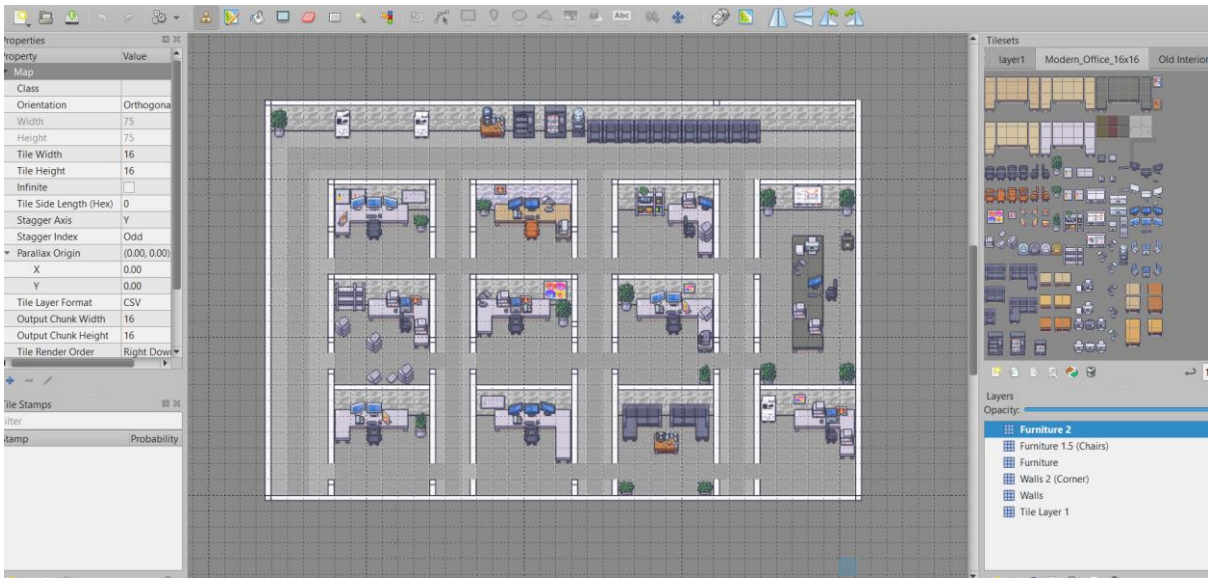

Figure 11 – Screenshot in "tiled", image of the Main Office map created with tileset.

- The map has a lot of space for both the player and NPCs to move about, the grid pattern for NPCs specifically. (Figure 17)
- The player has their own defined area/cubicle with the brown table and chair (Figure 10), where they perform computer related tasks.

Town

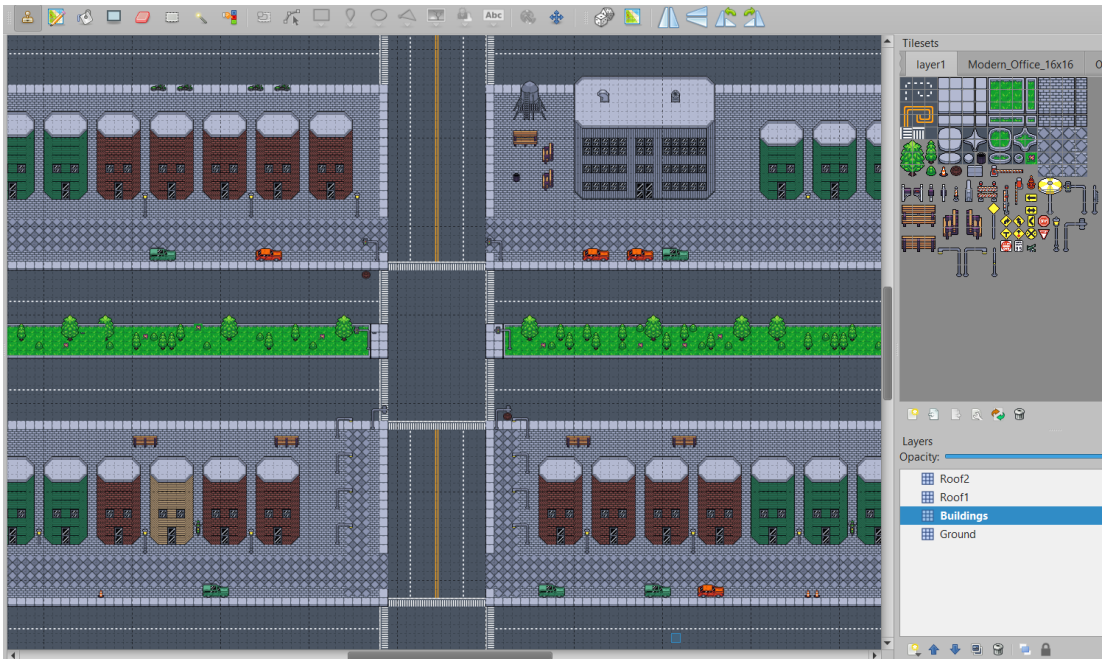

Figure 12 – Screenshot in "tiled", image of the "Town" map I created with a tileset.

- Large area for the player to walk around and speak to NPCs.
- Company building is on the top right-hand side (Figure 11).

4.5 Cybersecurity Threat Problem Statements and their Respective Mechanic

I simplified all cybersecurity issues into a problem statement.

- Problem: A person encounters a cyber threat or is at risk of making a mistake that can compromise their system or data. What causes this problem? Why is it a problem?
- Solution: The appropriate course of action to solving or preventing the problem.

The workspace, computer and NPCs were inspired by insider threats (Table 1) and physical breaches. These types of cyber-threat exist outside of the digital landscape, posing a threat to people that leave personal devices open in public spaces.

Problem – Insider Threats	Solution(s)
A malicious actor exists in the space where a person is using a device. This malicious actor could attempt to use the device if the person must leave it, for whatever reason. This can give them access to their private data.	Lock your device whenever you leave it if it cannot be moved (like a PC). Do not perform sensitive tasks while being watched.

Table 4 - Insider Threats Problem Statement

NPCs will walk around the office. If the player is not inside their workspace, and they leave their computer logged in, the player's computer will be breached, and they lose points. However, logging in and out will be slower than quick starting and closing, using up more of your time.

```
ComputerController()
SET isloggedin TO false

function login:
    SET isLoggedIn TO true
    WAIT x SECONDS
    OPEN COMPUTER

function logout:
    SET isLoggedIn TO false
    WAIT x SECONDS
    CLOSE COMPUTER

function quickstart:
    OPEN COMPUTER

function quickclose:
    CLOSE COMPUTER
```

Figure 13 – Pseudocode for the log in and log out system.

There must be reasons for the player to leave their area to allow them to practice logging out, so I planned a minigame where machines around the office would occasionally fail, and the player must fix them. Leaving machines broken for too long would make the player lose points.

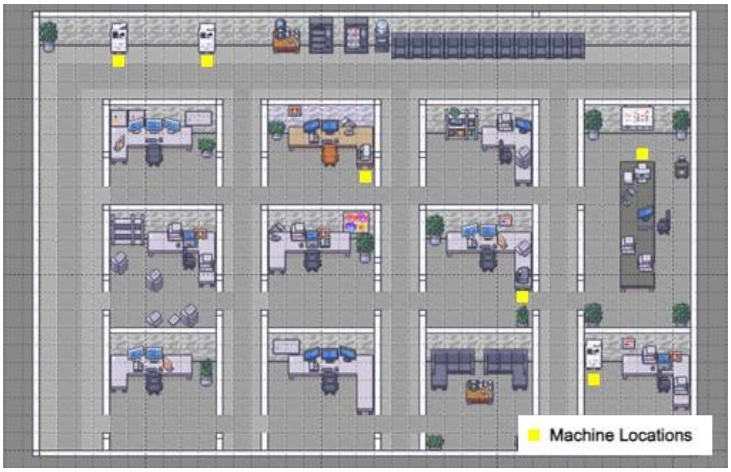

Figure 14 – Office marked with machine locations that must be fixed if broken.

The email system is the main gameplay mechanic. Players will receive several emails each day, and they must empty their inbox of emails to complete the day/level. The email concept was used to introduce phishing, social engineering and spoofing to the game (Table 1).

Problem – Phishing/Spoofing/Social Engineering	Solution(s)
Malicious actors are disguising their malware content as legitimate messages and emails. These messages can be deceptive in nature and could lead to me clicking on malware that compromises the system or reveals private data.	Pay attention to all content within a message, including the sender's email, link URLs, and other content within a message to determine its legitimacy. Use your knowledge of what legitimate messages look like to identify fake content.

Table 5 - Phishing/Spoofing/Social Engineering Problem Statement

.

The email system is designed to train players to decipher real content from fake. In-game, the company has a specific domain name (@corpo.com) that only real company emails will have. However, even real employees may send malware and other malicious content to the player, so they will need to understand the intent of the email. Players can either reply to or report emails.

Sender Email	Message	Correct Action
fjones@corpo.com	"Please enable two factor authentication here:"	**REPLY**
fjones@corpol.com	"Please enable two factor authentication here:"	**REPORT**
fjones@corpo.com	"Please send me your account details."	**REPORT**

Table 6 - Email Response Examples

This required me to create an email system that could create emails, display them on screen, and update the UI as the player answers emails.

Figure 15 – Mock-up of the Email System UI.

While most emails only require a reply, some emails will trigger an additional minigame. One of these is a minigame where the player composes a reply email and must attach the correct information to their response email, or else they will risk sending information to an incorrect receiver.

Another minigame that can be triggered is the **passcode scanner**. This mechanic introduces the concept of brute force attacks/password attacks into the game.

Problem – Brute Force Attacks	Solution(s)
Malicious actors are attempting to access my accounts by testing a multitude of passwords. They can gain access to my account if my password is guessed, however I must remember my password.	Use a combination of lower/upper case letters, symbols, and keys in the password. Avoid commonly used passwords and make the password a good length.

Table 7 - Brute Force Attack Problem Statement

The passcode minigame requires the player to enter a passcode of coloured symbols into a scanner to start scanning documents. After the scan is complete, the player must re-enter the password to access the documents.

The player loses points if:

- The password used two or less kinds of symbols or colours.
- The password was too short.
- They do not enter the correct password in three tries.

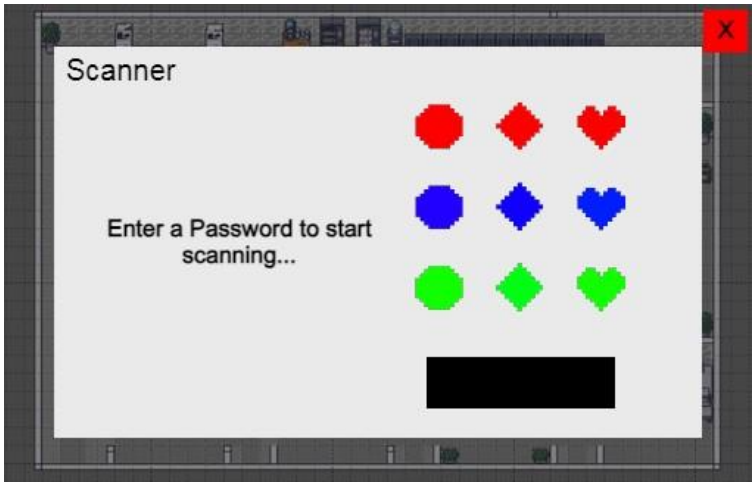

Figure 16 – Mock-up of the Scanner UI.

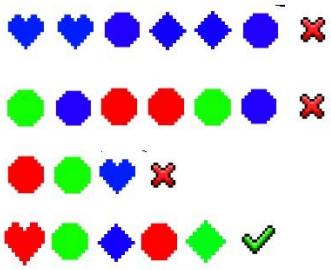

Figure 17 –Examples of good and bad passcodes.

Inspired by "Man in the Middle" attacks, the "**Wi-Fi Network**" mechanic will act as another distraction from the main goal of completing the email inbox.

Problem – Man in the Middle/Networks	Solution(s)
Many public networks are free to use, but many are also unsecure. It is possible for a third party to intercept my connection, and gain access to the data I send along the network.	Avoid using public or untrusted networks. Make sure you are always connected to a secured network, and

Table 8 - Main-in-the-Middle Attack Problem Statement

The strength of the company's network connection will falter throughout gameplay until it disconnects automatically. This will remove the player from the secured company network to an unsecure network. The player will lose points depending on how long they're connected to the unsecure network. However, they can re-connect to the company network when disconnected, or they can refresh the connection if it grows weak. However, reconnecting to the network will take a couple of seconds, so it should only be done when necessary.

4.6 Winning, Losing and Score System

Players will be rewarded points whenever they make a correct action, such as correctly responding to an email, correctly reporting phishing scams, using a strong passcode, and more. Players will lose points upon doing poor actions, such as incorrectly responding to emails, falling for phishing emails, leaving machines broken and more.

Mistakes will have different levels of severity. Mistakes of high severity will result in a game loss faster than mistakes of lower severity.

Severity	Action
Low-Medium	Creating a weak password, reporting harmless email, leaving a machine broken for a short time, etc.
High	Falling for phishing scam, reporting a real minigame email, leaving your computer un-guarded, forgetting the scanner code, etc.

Table 9 - Error Severity

The score manager will be able to identify different mistakes and deduct points accordingly. This will also give the system the potential to save the performance of the player for each level and save it to a database and use it to affect later sessions.

4.7 System Class Diagram

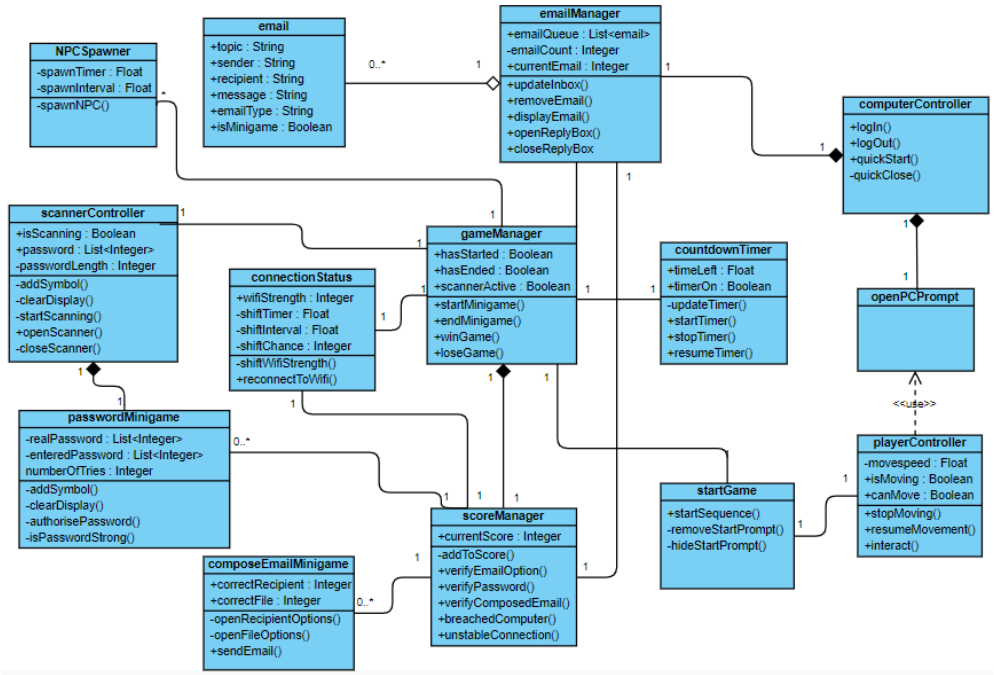

Figure 18 – Script Interaction Class Diagram.

"gameManager" tracks the state of the game, controlling when the game starts and ends. Starting the game triggers "countdownTimer" to start the timer, as well as "NPCSpawner" and "connectionStatus" to spawn NPCs and start the network respectively. The game manager uses "scoreManager" to determine if the player makes too many mistakes that require the game to end. The score manager is connected to any action that can reward or deduct points, including all the minigames and the email system. "emailManager" holds several emails for each level and will signal the game manager to end the game when it runs out of emails.

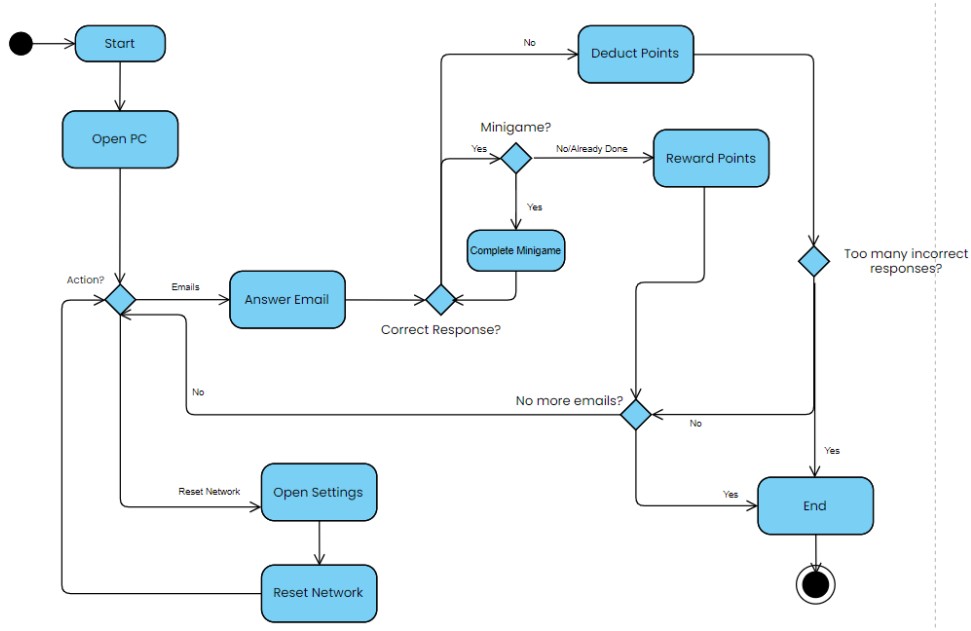

Figure 19 – Gameplay Activity Diagram.

The game starts when the computer is opened. The computer is primarily for answering emails, but if the Wi-Fi needs resetting, then the player can open settings to fix it. Upon answering an email, the player gains or loses points depending on the response. This continues until the player either makes too many mistakes in-game or they read all emails.

5 Implementation

5.1 Character Animations

Animations for both the player and NPCs use a blend tree that switches animations depending on the force being applied on the character/NPC objects (Figure).

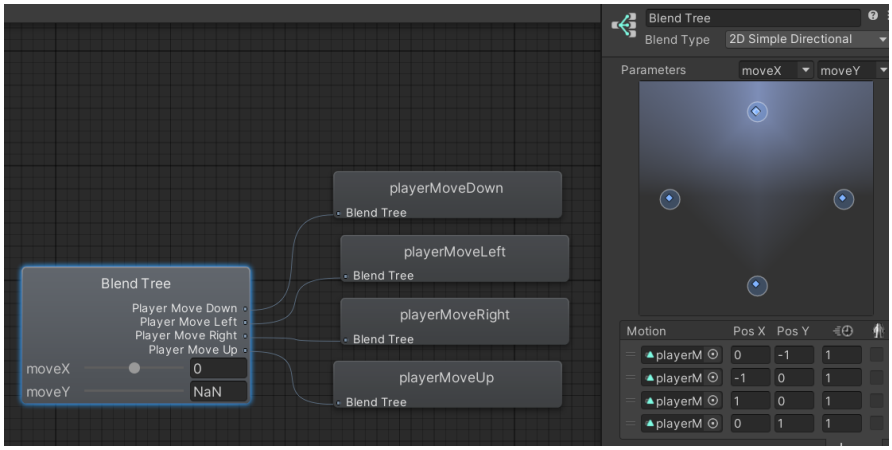

Figure 20 – Player Movement Blend Tree in Unity

```
myAnim.SetFloat("moveX", Input.GetAxisRaw("Horizontal"));
myAnim.SetFloat("moveY", Input.GetAxisRaw("Vertical"));
myAnim.SetBool("playerMoving", playerMoving);
myAnim.SetFloat("lastX", lastMove.x);
myAnim.SetFloat("lastY", lastMove.y);
```

Figure 21 – Code for the animator on the playerController object

"moveX" and "moveY" are variables for the animator that track which direction the player object is moving in cardinally, so the animator knows which walking animation to play. "lastX" and "lastY" track the last direction the player moved in, so when the player stops moving, the animator knows which direction the player/NPC should be facing while standing.

5.2 The Timer

The timer is a mechanic for building tension during gameplay. It increases the likelihood of failure but also trains players to recognize cyber threats under pressure.

Figure 22 – The timer UI object at the top of the screen in Unity.

The "countdownTimer" script takes an integer called "timeLeft" and it continuously decrements until it reaches zero or is stopped by the game manager. The game loss sequence is called if it reaches 0.

```
void Update()
{
    if(timerOn)
    {
        if(timeLeft > 0)
        {
            //decrement timer
            timeLeft -= Time.deltaTime;
            updateTimer(timeLeft);
        }
        else
        {
            Debug.Log("Time is UP!");
            timeLeft = 0;
            timerOn = false;
            theGameManager.endTheGameLoss();
        }
    }
}
```

Figure 23 – timer countdown functionality from the timer script

5.3 Game Mechanics: NPCs and the Office Area

There are two types of NPCs (non-player characters) in the game; regular NPCs and office NPCs. Regular NPCs are primarily for scenes outside of the office, they move around randomly, can have restricted movement zone, and will speak a line of dialogue if spoken to.

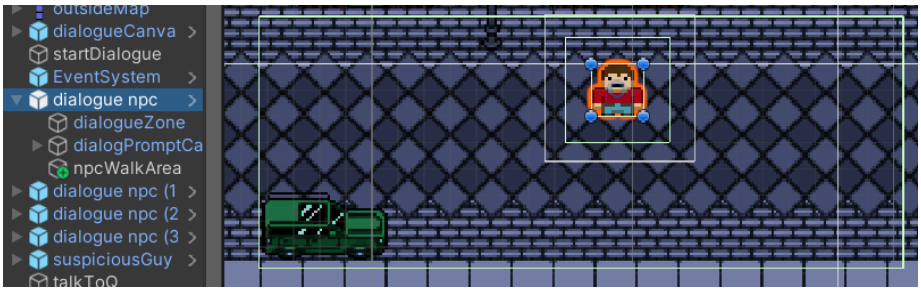

Figure 24 – NPC with a defined outer movement zone(npcWalkArea).

```
//npc moves in direction
switch(walkDirection)
{
    case 0:
        //up
        myRB.velocity = new Vector2(0, moveSpeed);
        lastMove = new Vector2(0, moveSpeed);
        if (hasWalkZone && transform.position.y > maxWalkPoint.y)
        {
            isWalking = false;
            waitCounter = waitTime;
        }
        break;
    case 1:
        //right
        myRB.velocity = new Vector2(moveSpeed, 0);
        lastMove = new Vector2(moveSpeed, 0);
        if (hasWalkZone && transform.position.x > maxWalkPoint.x)
        {
            isWalking = false;
            waitCounter = waitTime;
        }
        break;
```

Figure 25 – The zone restriction in the npcMovement script, for up and right.

If the NPC has a zone restriction, they will automatically stop moving once they reach the x or y limit and wait before choosing a new direction to move.

Office NPCs move around the office, following a grid pattern.

Figure 26 – Movement pattern for NPCs in the office.

Upon spawning, they move in a chosen direction. When an NPC reaches a node, they will choose a new direction depending on which direction is enabled within the node. Each node checks which directions it has enabled and will randomly choose from one of them. If no directions are enabled, the node will stop the NPC.

```
private string switchDirection()
{
    List<string> possibleDirections = new List<string>();

    // Add all possible movement directions to the list
    if (canMoveLeft)
    {
        possibleDirections.Add("left");
    }
    if (canMoveRight)
    {
        possibleDirections.Add("right");
    }
    if (canMoveUp)
    {
        possibleDirections.Add("up");
    }
    if (canMoveDown)
    {
        possibleDirections.Add("down");
    }

    // Check if there are any possible directions
    if (possibleDirections.Count == 0)
    {
        return "stop";
    }
    else
    {
        // choose random direction from list
        int chosenIndex = random.Next(possibleDirections.Count);
        return possibleDirections[chosenIndex];
    }
}
```

Figure 27 – switchDirection method on each node in the grid.

This results in a wave of NPCs that will take unique routes around the office.

Figure 28 – NPCs walking around the office randomly along the grid in Unity.

The player's area has a zone that tracks the people inside of it at any point in time. If an NPC enters the area while the player is not inside, and the computer is logged in, there is a 50% chance that the NPC will tamper with the computer, causing the player to lose points.

```
void OnTriggerEnter2D(Collider2D other)
{
    if(other.gameObject.tag == "Player")
    {
        inCubicle = true;
        Debug.Log("Entering Workspace...");
    }

    if(other.gameObject.tag == "NPC")
    {
        cubicleSum = cubicleSum + 1;
        npcInCubicle = true;
        Debug.Log("NPC entering Workspace...");

        //NPC attempts to tamper with users PC
        if(!inCubicle && theComputer.loggedIn)
        {
            int tamperChance = Random.Range(0,2);

            if(tamperChance == 1)
            {
                theScoreManager.vulnerablePC();
            }
```

```
void OnTriggerExit2D(Collider2D other)
{
    if(other.gameObject.tag == "Player")
    {
        inCubicle = false;
        Debug.Log("Exiting Workspace...");
    }

    if(other.gameObject.tag == "NPC")
    {
        cubicleSum = cubicleSum - 1;
        Debug.Log("NPC exiting Workspace...");
        if(cubicleSum <= 0)
        {
            npcInCubicle = false;
        }
    }
}
```

Figure 29 – TriggerEnter and TriggerExit scripts for the "playerOfficeCheck" script.

5.4 Game Mechanics: The Computer

The player can access the computer by walking into their chair and pressing space. This will disable their movement and open the computer UI.

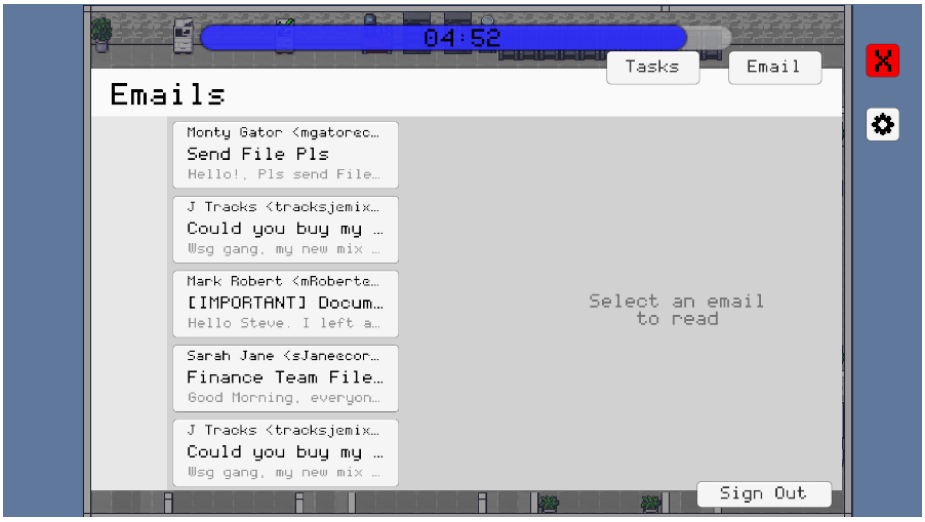

Figure 30– Screenshot of the computer UI in Unity, displaying the email screen.

The computer UI has five control buttons. The "Tasks" and "Email" buttons switch between the task screen and the email screen respectively. The red "X" icon instantly closes the computer, the gear icon below it opens the settings screen. The sign out button closes the computer after a few seconds.

```
public void logOut()
{
    //deactivate all other screens
    emailScreen.SetActive(false);
    taskListScreen.SetActive(false);
    systemScreen.SetActive(false);

    thePlayer.canMove = true;
    loggedIn = false; //only logging out sets this to false
    thePC.pcOpen = false;

    //play log out slider
    loadingBarController theSlider = loginSlider.GetComponent<loadingBarController>();
    theSlider.startLoading();
}
```

```
public void forceClose()
{
    thePlayer.canMove = true;
    computerScreen.SetActive(false);
    thePC.pcOpen = false;
}
```

Figure 31 - logout and forceClose functions in the computerController script.

While both the log out button and red "X" close the computer, the log out function must close all individual screens and call its slider to load completely before closing the screen fully (Figure 22). Quick closing is instant in comparison; however, it does not set "loggedIn" to false, leaving the computer vulnerable to NPCs (Figure 28).

5.5 The Email System

The email system is centralized around the "emailManager" class which holds a list of "email" objects.

```
public class email : MonoBehaviour
{
    //email structure
    public string emailTopic;
    public string emailSender;
    public string emailRecipients;
    public string emailMessage;

    //email answer options
    public string option1;
    public string option2;

    // 1 - best, 2 - good, 3 - bad, 4 - very bad
    public int option1Result;
    public int option2Result;
    public int reportResult;

    //type of cybersecurity issue
    //safe, malicious, phishing, spoofing
    public string emailType;

    //if the email is a minigame type of email
    public bool isMinigame;
    //password, compose-email
    public string minigameType;
```

Figure 32 - part of the "email" class.

The email class mimics real emails, having their own topic, sender, recipient, and message. The emailManager uses these strings to display the email information in both the preview and email body on the email page.

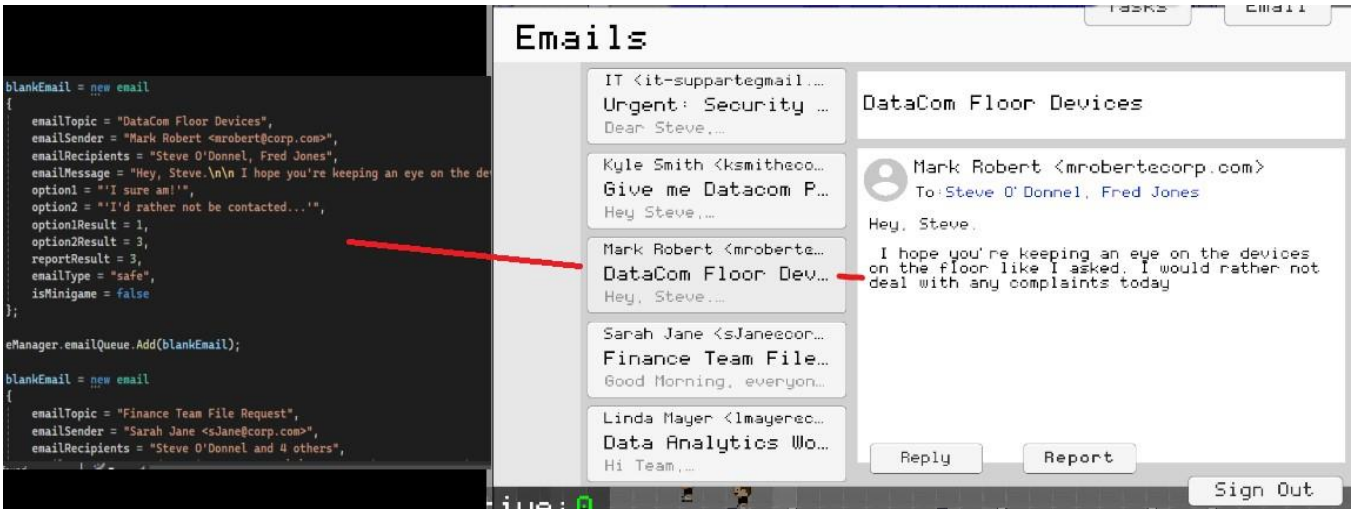

Figure 33 – email objects being created in C# and called to the email screen's UI in Unity.

Emails are added to the "emailQueue" list in the email manager in their respective order (you can see the email from Sarah below the email from Mark, Figure 33). All five email previews are buttons that display whichever emails are in the first five slots of the list. The list will update whenever an email is responded to, removing it from the list.

```
public void updateInbox()
{
    int backOfQueue;
    bool blankEntries = false;
    int queueLength = emailQueue.Count;

    if (queueLength < 5)
    {
        //ensure that there are always 5 emails
        backOfQueue = 5 - queueLength;
        blankEntries = true;

        for (int i = 0; i<backOfQueue; i++)
        {
            email blankEmail = new email
            {
                emailTopic = "",
                emailSender = "",
                emailRecipients = "",
                emailMessage = ""
            };

            emailQueue.Add(blankEmail);
        }
```

```
    //updating all buttons
    senderName1.text = emailQueue[0].emailSender;
    emailTopic1.text = emailQueue[0].emailTopic;
    emailBody1.text = emailQueue[0].emailMessage;

    senderName2.text = emailQueue[1].emailSender;
    emailTopic2.text = emailQueue[1].emailTopic;
    emailBody2.text = emailQueue[1].emailMessage;

    senderName3.text = emailQueue[2].emailSender;
    emailTopic3.text = emailQueue[2].emailTopic;
    emailBody3.text = emailQueue[2].emailMessage;

    senderName4.text = emailQueue[3].emailSender;
    emailTopic4.text = emailQueue[3].emailTopic;
    emailBody4.text = emailQueue[3].emailMessage;

    senderName5.text = emailQueue[4].emailSender;
    emailTopic5.text = emailQueue[4].emailTopic;
    emailBody5.text = emailQueue[4].emailMessage;
```

Figure 34 – parts of "updateInbox" method in "emailManager".

When there are less than 5 emails in the list, the UI is updated to have blank emails for the remaining preview buttons (Figure 34). The blank emails are removed after the UI updates. Emails have three possible responses, two reply options and report. These three options have an assigned number that determines if it's correct or not, and to what extent (Figure 33). The player gains or loses points depending on the options assigned number (Figure 35).

```
public void chooseOption2()
{
    //options rated 1 or 2 are good
    if(eManager.emailQueue[currentIndex].option2Result <= 2)
    {
        Debug.Log("Good Answer!");
        addScore(100);
    }
    //options rated 3 or 4 are bad
    else if(eManager.emailQueue[currentIndex].option2Result > 2)
    {
        Debug.Log("No...");
        addScore(-50);
        tenStrikes += 1;

        if(eManager.emailQueue[currentIndex].option2Result == 4)
        {
            fourStrikes += 1;
        }
    }
    eManager.removeEmail();
}
```

Figure 35 – "chooseOption2" method in "scoreManager".

Some emails are marked as minigames using the "isMinigame" boolean variable (Figure 33). When answered correctly, they trigger an additional action that is required to answer the email. One of these is an email composition minigame.

Figure 36 – "compose-email" emailType and the reply screen UI in Unity.

This type of email has more attributes and opens a new screen (Figure 36). The player must create a response by choosing the correct recipients and the correct attachment. They lose points if either of the fields are incorrect.

The email system is dependent on using integer values to represent what the player is selecting. The main challenge came from ensuring that the front end UI was always synchronized with the back end whenever a new email was clicked, when an email was removed, when the player closed the computer and more.

5.6 Game Mechanics: Passcode Scanner

Emails with an "emailType" of "password" activate the passcode minigame. The player must walk over to the scanner object in the office and interact with it. This opens the scanner's UI.

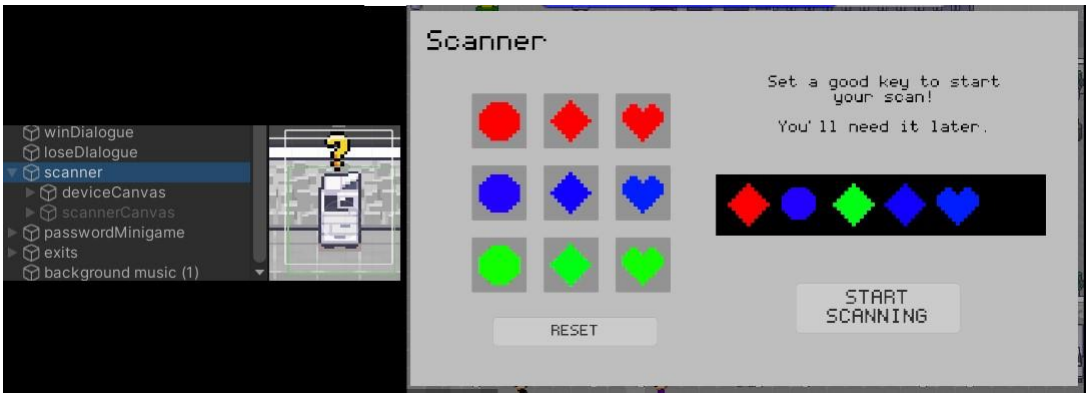

Figure 37 – Scanner object on the map and Scanner UI in Unity.

The player will be prompted to enter a passcode to start the scanning process, which will take ~15 seconds of loading to complete, incentivizing the player to leave the scanner and perform another task while it loads. After the scanner finishes scanning, the player can re-open the UI and they must re-enter the passcode they created. The player has three attempts to enter the passcode correctly, however, this passcode will also be evaluated upon being guessed.

Each symbol has a corresponding integer value, and the player's entered passcode is saved once scanning begins. For example, the password in Figure 37 would be saved as "2,4,8,5,6" in the list that defines the password (Figure 29).

```
//9 symbols for passwords
// 1 - Red Circle / 2 - Red Diamond / 3 - Red Heart
// 4 - Blue Circle / 5 - Blue Diamond / 6 - Blue Heart
// 7 - Green Circle / 8 - Green Diamond / 9 - Green Heart
switch (symbolNumber)
{
    case 1:
        //red circle
        switch (passwordLength)
        {
            case 0:
                newKey = Instantiate(redCircle, passKey1.transform);
                break;
            case 1:
                newKey = Instantiate(redCircle, passKey2.transform);
                break;
            case 2:
                newKey = Instantiate(redCircle, passKey3.transform);
                break;
            case 3:
                newKey = Instantiate(redCircle, passKey4.transform);
                break;
            case 4:
                newKey = Instantiate(redCircle, passKey5.transform);
                break;
            case 5:
                newKey = Instantiate(redCircle, passKey6.transform);
                break;
        }
        break;
```

Figure 38 – Values for each symbol and switch statement that adds symbols to the passcode on the UI, in scannerController.

The "addSymbol" method adds the symbol to the UI and adds its corresponding number to the password being created. The "passwordLength" switch statement ensures that the program displays the passcode symbols in their proper order on the scanner UI.

The evaluation of a password uses four criteria: password length, shape diversity, colour diversity and simple sequence checking. For length, the program checks if the password length is longer than 3. For colour/shape diversity, symbols are grouped by colour and shape: (Red:1,2,3)(Blue:4,5,6)(Green:7,8,9)(Circle:1,4,7)(Diamond:2,5,8)(Heart:3,6,9). The password must include more than one kind of colour and shape, and the program checks how many of these groups are present within the password.

```
foreach (int number in password)
{
    if ((number == 1 || number == 2 || number == 3) && redFound == false)
    {
        redFound = true;
        coloursTotal = coloursTotal + 1;
    }
    else if ((number == 4 || number == 5 || number == 6) && blueFound == false)
    {
        blueFound = true;
        coloursTotal = coloursTotal + 1;
    }
    else if ((number == 7 || number == 8 || number == 9) && greenFound == false)
    {
        greenFound = true;
        coloursTotal = coloursTotal + 1;
    }
}
```

Figure 39 – For loop for "colourCount" method in the "passwordMinigame" class.

Simple sequence checking checks if the password is made of a simple iterating sequence of numbers.

```
private bool isSimpleSequence(List<int> password)
{
    // Check if the password is a simple sequence of numbers
    for (int i = 0; i < password.Count - 1; i++)
    {
        if (password[i] + 1 != password[i + 1])
        {
            return false;
        }
    }
    return true;
}
```

Figure 40 – isSimpleSequence method in the "passwordMinigame" class.

All these criteria are sent to the score manager, and the player loses points if the password does not pass all the criteria.

5.7 Game Mechanics: Wifi Network

The network mechanic is automatic and begins when the game starts. The connection value ranges from 5 to 1, 5 being a strong connection and 1 being a weak connection. If the connection value is at 1 for too long, it will reach 0 and the player will automatically connect to an unsecure network. The player will start to lose points as they remain connected to the unsecure network.

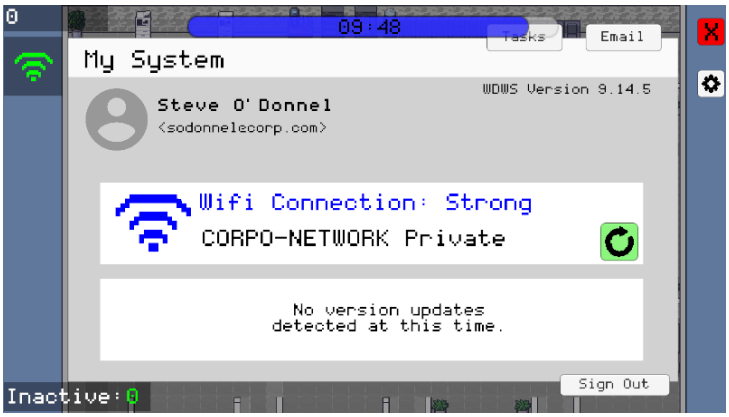

Figure 41 – System setting screen UI.

Players can see the connection strength on both the settings screen and the Wi-Fi icon on the left (Figure 41). They can refresh the connection if it becomes weak.

```
shiftChance = Random.Range(0,100);
//check conenction value
switch(connectVal)
{
    case 5://100% chance of going down, grace period after reconnecting
        connectVal -= 1;
        break;

    case 4://50% chance of staying, 50% chance of going down
        if (shiftChance <= 49)
        {
            //no change
        }
        else
        {
            connectVal -= 1;
        }
        break;
```

Figure 42 – Part of the "wifiShift" method in the "systemStatus" class.

The connection value has a different chance to shift at each level. The value can either go up, stay the same or go down. The chance of the former two outcomes happening decreases as "connectVal" decreases, and the chance of the latter outcome happening increases as "connectVal" decreases.

Figure 43 – Settings UI at connection values 3 to 0.

5.8 Other Mechanics

Figure 44 – Screenshot of the game in Unity.

Broken machines in the game are marked with both an "x" symbol on the map, and an overall count on the player's HUD (Figure 44). They have a random chance of breaking throughout gameplay; the player fixes them by walking to them and interacting with them.

5.9 Game and Level Structure

The game introduces new mechanics in each level, trickling them in before reaching the final levels where all of them are enabled. Character dialogue is used to introduce these mechanics to the game and inform the player on how to tackle them.

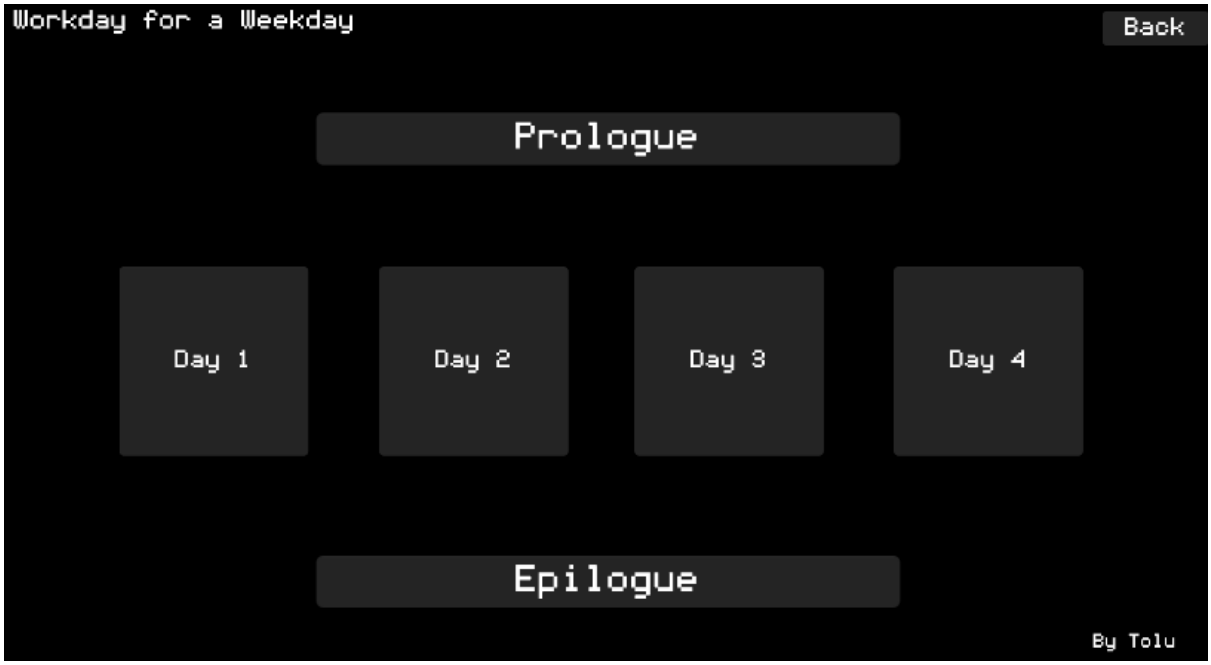

Figure 45 – Screenshot of the level menu in Unity.

Level	Mechanics Included
Day 1	Email System
Day 2	Email System, Machine Maintenance, Compose Emails
Day 3	Email System, Machine Maintenance, Compose Emails, Passcode Scanner, Wi-Fi Connection
Day 4	Email System, Machine Maintenance, Compose Emails, Passcode Scanner, Wi-Fi Connection

Table 10 - Mechanics for each Level

The prologue and epilogue are purely storyline elements that start and finish the story of the game.

The plot of each day is as follows:

Level	Plot
Prologue	"Steve wakes up to a call from a recruiter, asking him to visit the "Corpo" building. Upon reaching the building, he is called into the owner's office. Steve meets the owner of the building, Mark Robert, and is hired on the spot into the Data and Communications team. Upon walking home, a mysterious man called Q warns Steve about Corpo and its hostile work environment."
Day 1	"On Steve's first day, he is introduced to the rest of the Datacom team, including his line manager, Fred. Fred shows Steve around the office, and Steve works his first shift at Corpo. At the end of the day, he speak with Q about how things went. Q explains to Steve the dangers of sharing personal emails with strangers."
Day 2	"Steve attends his second daily meeting, where the team finds out that the machines on their floor have been tamped with using a USB. Mark assigns Steve the role of keeping the Datacom's machines working, because employees from other departments will start entering the office to use them. At the end of the day, Steve speaks with Q again, and Q tells him why it's important to log out of devices when you leave them in public settings."
Day 3	"Corpo suffers a massive data breach. Many company accounts have been breached, and the buildings Wi-Fi has become unstable. Everyone is on edge, but Mark waves it off and blames the IT department. Fred teaches Steve how to use the scanner. Steve speaks with Q at the end of the day once more, Q suggests that the company is beginning to topple over."
Day 4	"Steve arrives at Corpo to find out that half of all employees quit overnight. Steve and Fred are forced to take over the work that the rest of the Datacom team left behind when they quit. By the end of the day, Steve and Fred also decide to quit, leaving Mark and Corpo behind to crash and burn. Steve talks with Q on his way home one final time. Q reveals his history as an IT specialist at Corpo and talks about how he lost his job due to the hostile environment."
Epilogue	"Steve gets a call from Fred to come visit the Corpo building. Upon arriving in the meeting room, Fred tells Steve about how Mark was fired by the regional manager of Corpo due to his poor management. Fred offers Steve his role back, and promises to run the company properly, as he had been promoted to owner. Fred also reveals that he hired a cybersecurity specialist to teach everyone proper cybersecurity etiquette and habits, and that specialist is none other than Q."

Table 11 - Plot for each Level

6 Testing

6.1 Unit Testing

Unit testing was the method I undertook to test the game. This was the most suitable method as it allowed me to test parts of the system as they were being implemented; issues could be found earlier into development. Due to how many individual parts of the system interact; it is important that they function well individually.

Character Animations

Test No.	Test Description	Expected Result	Actual Result
1	Press 'S' key to walk down.	Loop 'playerMoveDown.anim'	Looped 'playerMoveDown.anim'
2	Press 'W' key to walk up.	Loop 'playerMoveUp.anim'	Looped 'playerMoveUp.anim'
3	Press 'A' key to walk left.	Loop 'playerMoveLeft.anim'	Looped 'playerMoveLeft.anim'
4	Press 'D' key to walk right.	Loop 'playerMoveRight.anim'	Looped 'playerMoveRight.anim'
5	Stop moving down and face downwards.	Loop 'playerFaceDown.anim'	Looped 'playerFaceDown.anim'
6	Stop moving up and face up.	Loop 'playerFaceUp.anim'	Looped 'playerFaceDown.anim'
7	Stop moving left and face left.	Loop 'playerFaceLeft.anim'	Looped 'playerFaceDown.anim'
8	Stop moving right and face right.	Loop 'playerFaceRight.anim'	Looped 'playerFaceDown.anim'

Table 12 - Character Animation Unit Test

The walking animations worked, but the standing animations all defaulted to the facing down animation. This was shortly fixed upon tweaking the player movement controller to properly track which direction the player last moved in.

Email System Indexing and Email Queue

Purpose: To evaluate the synchronization between the email systems UI and the index of the email list, "emailQueue", in emailManager.

Test No.	Test Description	Expected Result	Actual Result
1	Test the email manager's ability to track which email in the list is being read. (e.g. clicking the 4th email preview button will set currentEmail to 3)	"currentEmail" value will change upon clicking an email button, according to its order.	"currentEmail" value changes upon clicking an email button, according to its order.
2	Test the email screen's ability to properly represent the current order of the email list in the email manager.	The email screen will display the information of the first five email objects in "emailQueue", in order.	The email screen displays the information of the first five email objects in "emailQueue", in order.
3	Test the email screen's ability to properly update the UI to represent changes to the email manager's list.	The email screen is updated every time an email is answered, and the correct email is removed from the UI.	The email screen is updated every time an email is answered, and the correct email is removed from the UI.
4	Test the email screen's ability to handle a list with less than 5 emails.	The email screen makes the remaining buttons blank. Blank buttons cannot be clicked.	The email screen makes the remaining buttons blank. Blank buttons cannot be clicked.

Table 13 - Email Manager and Email Screen UI Unit Test

The email screen and the email manager are in perfect synchronization. The UI always understands what the list in email manager looks like and displays it accordingly. The manager always knows which email the player is currently viewing.

Email Responses

Purpose: To check if email responses are properly being awarded/penalized.

Test No.	Test Description	Expected Result	Actual Result
1	Testing reply option for a safe email (reply is assigned 1/2)	Player will gain points upon clicking reply on a safe email.	Player gains points upon clicking reply on a safe email.
2	Testing report option for a safe email (report is assigned 3/4)	Player will lose points upon clicking report on a safe email.	Player loses points upon clicking report on a safe email.
3	Testing reply option for a malicious email (reply is assigned 3/4)	Player will lose points upon clicking reply on a malicious email.	Player loses points upon clicking reply on a malicious email.
4	Testing report option for a malicious email (report is assigned 1/2)	Player will gain points upon clicking report on a malicious email.	Player gains points upon clicking report on a malicious email.

Table 14 - Email Response Unit Test

The score manager properly adds and removes from the player's score tally to accurately reward appropriate email responses and punish inappropriate responses.

Passcode Evaluation

Purpose: To test if passcodes typed into the scanner have their strength evaluated appropriately. (Key: XX = colour/shape) (R = Red, B = Blue, G = Green, C = Circle, D = Diamond, H= Heart)

Test No.	Test Description	Expected Result	Actual Result
1	Testing the long password requirement (Code Entered: RC, BD, GH)	Passcode will be recognised as weak due to being short.	Passcode is recognised as weak due to being short.
2	Testing the diverse colour requirement (Code Entered: RC, RD, RD, RC, RH, RC)	Passcode will be recognised as weak due to lack of colour diversity.	Passcode is recognised as weak due to lack of colour diversity.
3	Testing the diverse shape requirement (Code Entered: RC, BC, RC, GC, GC, BC)	Passcode will be recognised as weak due to lack of shape diversity.	Passcode is recognised as weak due to lack of shape diversity.

4	Testing the simple sequence penalty (Code Entered: RC, RH, RD, BC, BH, BD)	Passcode will be recognised as weak due to the simple sequence.	Passcode is recognised as weak due to the simple sequence.
5	Testing a passcode that is strong (Code Entered: RC, BD, GH, BC, RD)	Password will be recognised as strong.	Password is recognised as strong.

Table 15 - Passcode Evaluation Unit Test

The passcode game manager was able to enforce all of its requirements appropriately and signalled the score manager to add or subtract points accordingly.

Game State Management

Purpose: To test the game manager's ability to interact with the rest of the system, testing its ability to trigger events upon game start, events upon the game ending, and to recognise when the game ends and under which conditions.

Test No.	Test Description	Expected Result	Actual Result
1	Testing the game manager's ability to recognise when the level has been won (all emails answered).	Once "emailQueue.Length" reaches 0, the game ends, the timer stops, and the player wins the level.	Once "emailQueue.Length" reaches 0, the game ends, the timer stops, and the player wins the level.
2	Testing if the player loses when the timer reaches 0.	When the timer reaches 0, the game ends and the player loses.	When the timer reaches 0, the game does not end.
3	Testing if the game ends when the player makes too many mistakes.	Upon incorrectly replying to four phishing emails, the time stops, the game ends and the player loses.	Upon incorrectly replying to four phishing emails, the time stops, the game ends and the player loses.
4	Testing if NPCs start to spawn only when the game starts.	When the game begins, NPCs start to spawn in the office and walk around.	When the game begins, NPCs start to spawn in the office and walk around.
5	Testing if the Wi-Fi begins to shift only when the game starts.	The script for Wi-Fi does not run until the timer start.	The Wi-Fi script starts when the player enters the office.

Table 16 - Game Manager Unit Test

The system was mostly synchronized, however, there were some disconnects between the timer, game manager and Wi-Fi script. The “countdownTimer” script did not call the “endGameLoss” method from the game manager, and the “systemStatus” script used to shift the Wi-Fi strength was not given the condition to only start counting towards the next shift when the game started. Both issues were recognized and fixed promptly.

These are only a few of the unit tests taken for the system. Most of them were done as the code was being written.

7 Evaluation

An open invitation to partaking in my research was sent on social media, and I was able to get six participants total. These participants took a survey prior to playing, played the entire demo, and then took a second survey after experiencing the game. My aim through this was to measure any improvement in cybersecurity knowledge, as well as interest built in the subject through story aspect and/or gameplay aspects.

7.1 Pre-Gameplay Evaluation

Question: "How would you rate your overall knowledge of Cybersecurity?"

Participant Num	**Value (1-10)**
Participant 1	4.00
Participant 2	6.00
Participant 3	5.00
Participant 4	4.00
Participant 5	6.00
Participant 6	8.00
AVERAGE	**5.50**

Table 17 - Cybersecurity Knowledge Pre-Game Ratings

The average score indicate that participants perceive themselves to have an overall moderate understanding of cybersecurity. They are neither completely unfamiliar with the topic, nor do they consider themselves experts. The populations standard deviation is 1.38, suggesting that while there is a slight spread of how participants rate their knowledge, most participants score close to the average. Given that no participant has complete confidence in their knowledge (9, 10), there is clearly room for improvement.

Question: "Have you taken any cybersecurity training?"

Participant Num	**Received Training?**	**Training Form**
Participant 1	No	N/A
Participant 2	Yes	Online Course
Participant 3	Yes	Formal Education/Training
Participant 4	No	N/A
Participant 5	Yes	Other
Participant 6	Yes	Formal Education/Training

Table 18 - Prior Cybersecurity Training Responses

Despite over 60% of participants claiming to have prior training in cybersecurity in some form, self-rated knowledge for cybersecurity is still very average. Naturally, the participants with no

form of training consistently reported a slightly below average rating. However, trained individuals only have an average rated understanding of 6.25. This is not a notable improvement from the entire population's average, only a ~13% increase overall. Despite a somewhat diverse history with their prior training, these methods did not create a significant amount of confidence in cybersecurity knowledge overall. This could potentially be attributed to these programs failing to make the information easy to retain over an extended period.

Cybersecurity confidence and habits

Question: "How would you rate your overall confidence in recognising cyber threats in any scenario?"

Participant Num	**Confidence Rating (1-10)**
Participant 1	6.00
Participant 2	6.00
Participant 3	6.00
Participant 4	6.00
Participant 5	8.00
Participant 6	6.00
AVERAGE	**6.33**

Table 19 - Cybersecurity Threat Recognition Confidence Ratings

There is even less variance in these results compared to the overall rating for cybersecurity knowledge. On average, participants feel more confident in recognising cyber threats than their overall knowledge of the topic. However, most participants only rated their understanding to be slightly above average, showing room for improvement.

Question: Which of these terms for cyber-attacks/threats could you recognise if you were faced with them?

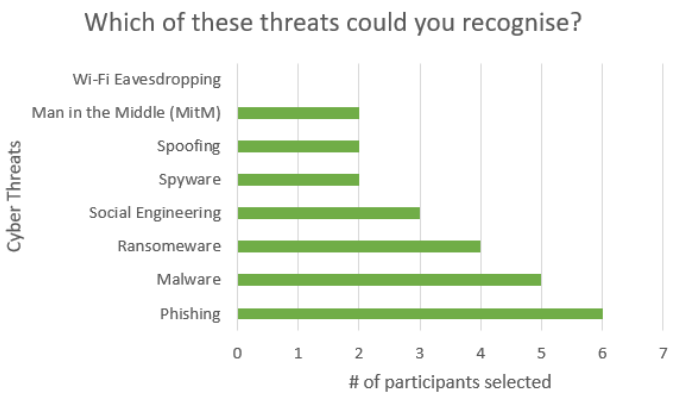

Figure 46 - Threat recognition results Bar Chart

Participants overall believe that they can recognise many of the most common threats. Phishing attempts are recognisable by every participant, with malware and ransomware following behind. This is expected, considering these types of attacks are the most commonly reported methods of attack in recent years and in general (Fortinet 2023)(Checkpoint 2023). Participants were not as confident in recognising network related attacks such as Man-in-the-Middle and Wi-Fi Eavesdropping, which are not as common as the formerly mentioned threats. Social engineering sits in the middle, only 50% of participants are confident in recognising social engineering attempts.

Question: "Who do you think poses a threat to cyber security (Select all that apply)"

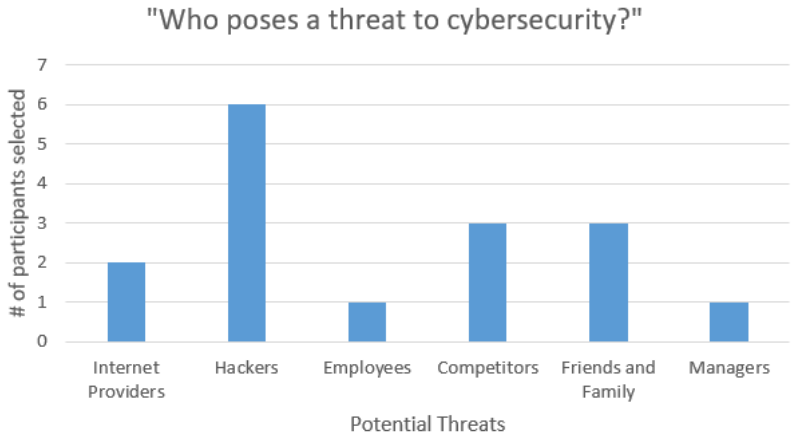

Figure 47 - Cybersecurity threat recognition Bar Chart

All participants were able to correctly recognise hackers as threats to cybersecurity, which was expected. However, all other correct answers including Employees, Competitors, Friends and Family, were only recognised by 50% of participants at best. This question was designed to test the understanding of where cyber threats can rise from. Participants overall do not completely understand that even non-malicious actors can act as threats unintentionally, and the fact that trusted actors have the potential to abuse trust to breach data (Employees, Friends and Family). The only participant to correctly recognise every potential bad actor was the participant with former training that rated their cybersecurity knowledge an 8.

Question: "When you notice an update to a piece of software/application/device, how long does it usually take you to update it?"

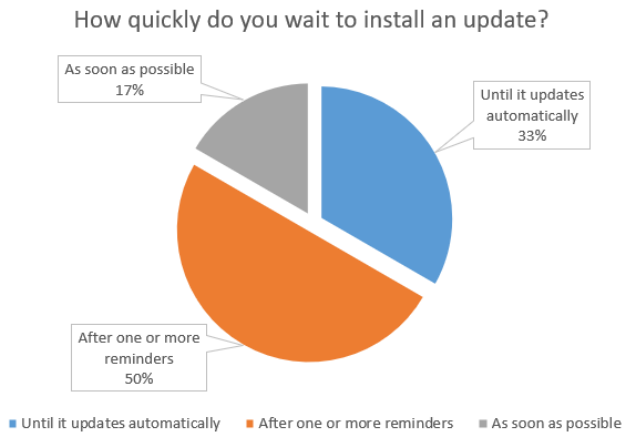

Figure 48 - Install updates question Pie Chart

Question: "Do you use different passwords for different online accounts? (Excluding minor variations of the same password as different)"

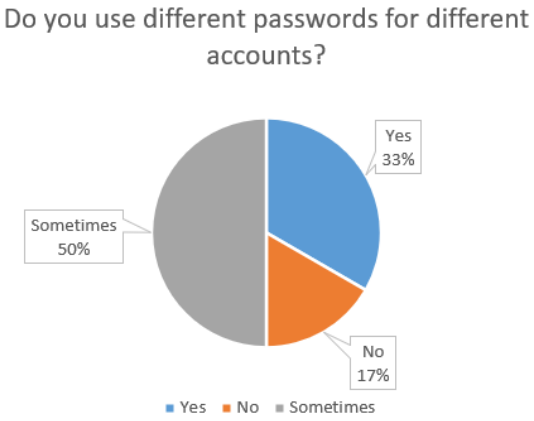

Figure 49 - Password habits Pie Chart

Only a singular participant has the proper habit of updating outdated software immediately when prompted, and only ~33% of participants had the proper habit of using completely different passwords for all their accounts.

This reveals a lack of understanding of where cyber-threats originate from, implying that most of the participants take a reactive approach to cybersecurity; only responding when the threat is in front of them instead of recognising potential threats. Most participants do not have proper cybersecurity habits; their habits are the kind that lower the defences of a system, leaving them vulnerable to malware and other threats that can go under the radar. This mirrors the reports of employers believing over half of their employees lack cybersecurity awareness, even with a large population of trained individuals (Fortinet, 2023).

Measuring Interest

Question: "How important do you think cyber security is in your daily life?"

Participant Num	Importance Rating (1-5)
Participant 1	5.00
Participant 2	3.00
Participant 3	5.00
Participant 4	5.00
Participant 5	4.00
Participant 6	5.00
AVERAGE	**4.50**

Table 20 - Cybersecurity Importance Ratings

Question: "How likely are you to willingly interact with learning material, outside of education, work and/or any other necessary scenario?"

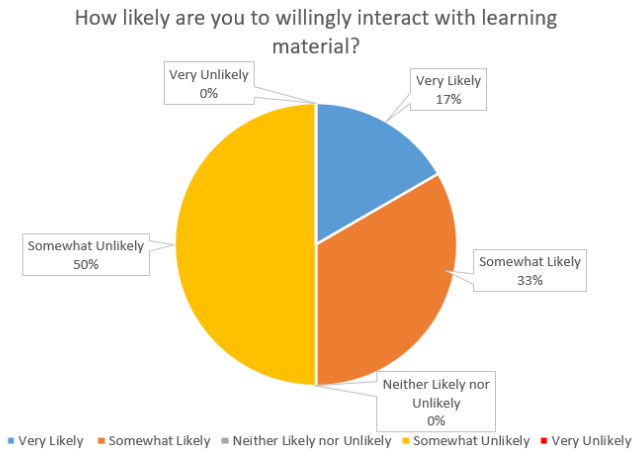

Figure 50 - Cybersecurity learning willingness Pie Chart

Participants strongly recognise that cybersecurity is important for their daily lives, yet they are not enthusiastic about interacting with learning material regarding the topic outside of mandatory scenarios.

Question: "What is your most preferred method of learning?"

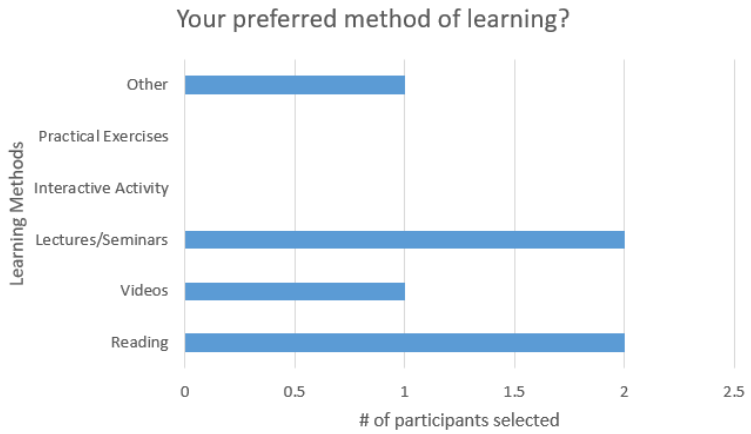

Figure 51 - Method of learning Bar Chart

I also observed that participants preferred the traditional methods of learning (Reading, Lectures and Seminars) over less conventional means (Interactive activities and practical exercises). This may refer more to academic learning rather than awareness campaigns and such.

These pre-gameplay results gave me an indication of where my participants were at in terms of overall cybersecurity knowledge, habits, and interest in the topic. While participants believe they have a solid understanding of avoiding threats, their habits still expose clear gaps in knowledge regarding threats that are still common but are not as common as phishing and malware. Participants unanimously understand how important cybersecurity is, but 83% of them do not have a sense of urgency to learn about the topic outside of when it is mandatory; 50% of participants being straight up unlikely to pick up the topic out of their own volition. This could either be because they believe that they understand the topic well enough (which evidently is not true for everyone), or their interest in the topic has not been developed.

7.2 Post-Gameplay Evaluation

Cybersecurity confidence and habits

Question: "How would you now rate your overall knowledge of cyber security?"

Participant Num	Pre-Game Rating	Post-Game Rating	Increase (%)
Participant 1	4.00	7.00	+75.00%
Participant 2	6.00	6.00	+0.00%
Participant 3	5.00	8.00	+60.00%
Participant 4	4.00	8.00	+100.00%
Participant 5	6.00	7.00	+16.67%
Participant 6	8.00	8.00	+0.00%
AVERAGE	**5.50**	**7.33**	**+33.27%**

Table 21 - Pre- and Post- Game Ratings

Overall, after playing the game, the overall participant rating of cybersecurity knowledge increased to 7.33/10. Cybersecurity knowledge increase by ~33%. However, the results also show a split within the participants. The greatest increases were seen in participants that, pre-gameplay, did not feel as confident in their cybersecurity knowledge. Participants with higher pre- gameplay scores did not improve a significant amount, if at all.

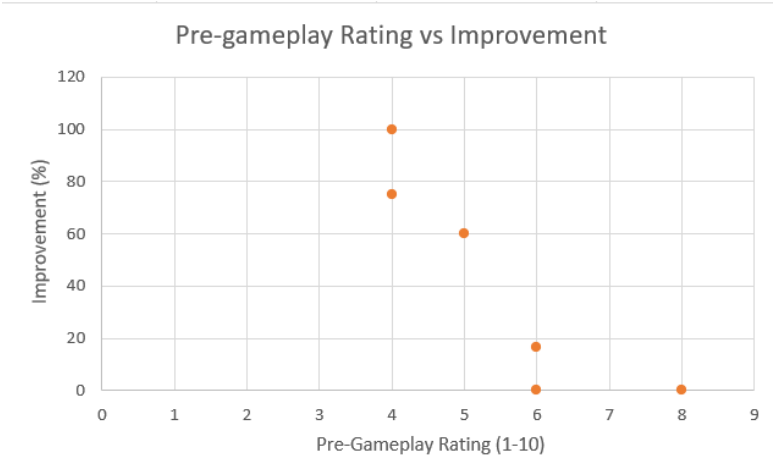

Figure 52 - Pre-game rating - improvement% Line Graph

These two factors create a negative correlation. This implies that the game was better at informing the less knowledgeable, and likely did not introduce many new concepts to the more knowledgeable participants. This is supported by the fact that responses were perfectly split between yes and no when answering "Do you believe that your understanding of cyber security concepts has improved?". This divide leads me to believe that the game could not match up to the informative nature of formal cybersecurity education or courses, of which the educated portion of the participants took part in.

Question: "Which threats do you feel more confident in identifying/recognising and defending against?"

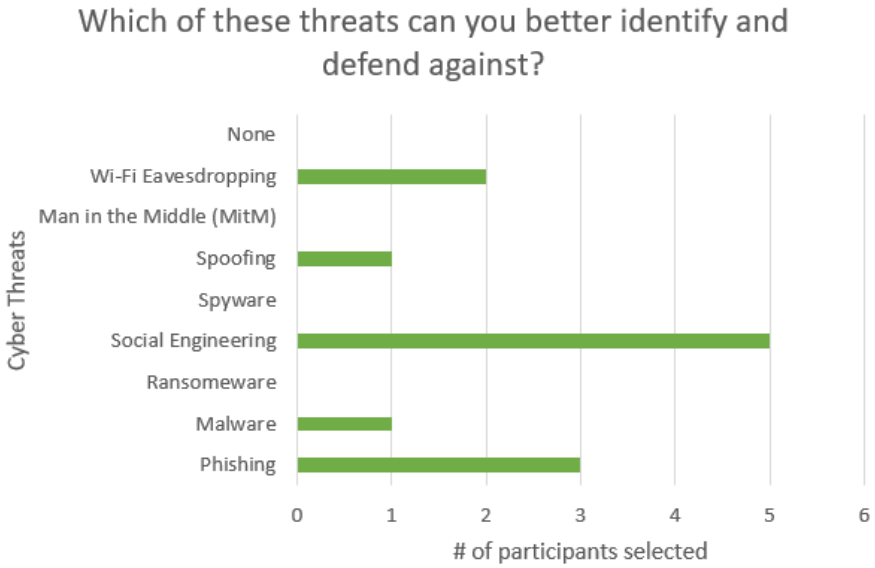

Figure 53 - Threat Identity Bar Chart

Despite the split in how many participants felt it terms of knowledge improvement, every participant felt more confident in identifying one or more types of cyber threats. This is partially confusing; however, I believe that it represents the difference between the game's ability to teach versus its ability to train. Experienced participants may have not been introduced to any new concepts regarding what threats are and how to deal with them, but their constant exposure to the concepts has improved their ability to identify threats.

Out of all the threats listed, social engineering stood out as the threat that almost every participant believed they could detect to an improved degree. This is likely due to how prevalent social engineering is to the story of the game and a lot of the dialogue. Perhaps this reveals that the story was the most informative part of the game. Phishing was the second most selected answer, likely due to how gameplay revolved around the email system; the main objective during each level being to decipher the intent of incoming emails. Considering every participant already felt confident in detecting phishing attempt pre-gameplay, the game likely allowed them to continuously test their ability to detect these attempts.

The only threat that was present in the game yet did not see any improvement was man-in-the-middle attacks. However, this threat is heavily related to Wi-Fi eavesdropping, so it is more likely that the game did not give this attack a distinct identity.

Question: "Who do you think poses a threat to cyber security? (Select all that apply)"

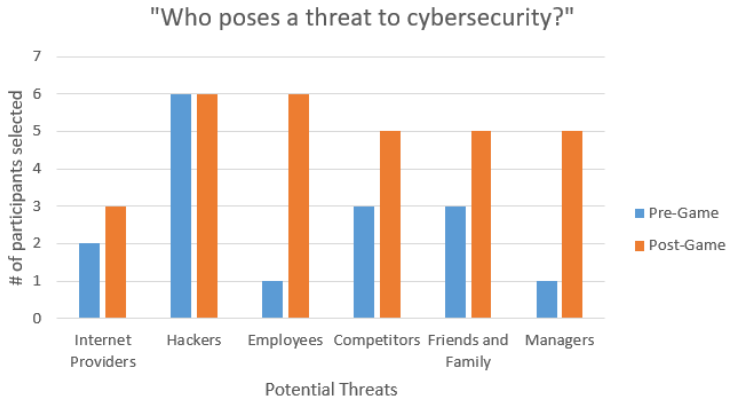

Figure 54 - Threat Identification comparison Bar Chart

This is the survey question that saw the most improvement compared to every other question. Nearly every participant was correctly able to identify employees, managers, competitors, friends, and family as potential threats to cyber security. This is despite half of them or less considering them threats beforehand. This supports the idea that the story was the most integral part of the game when it came to spreading awareness; the story used the idea of a *competitive* environment where *employees* would sabotage machines, and with a company *owner/manager* that enabled this behaviour. The topic of friends and family was not even present in the game, but it is likely that this concept of viewing any person as a threat, intentional or not, had influenced participants into thinking differently about the question.

Question: "Which aspect of the game challenged your attention and awareness the most, if any? How did it impact your learning experience?"

P. No	Responses
1	"Reading emails in a strict time limit"
2	"Failing allows us to recall our actions and try our best to prevent making mistake thus making this effective for learning."
3	"The printers and always having to sign out."
4	"multitasking between monitoring the office equipment while needing to quickly asses and reply to emails"
5	"Remembering to sign out of your account when you leave your seat. It reminded me that I am not in a friendly environment and to stay sharp.,"
6	"Switching my focus from emails to the wifi to the scanner made things hard to remember"

Table 22 - Awareness and Attention Challenge Responses

Many participants found the multi-tasking nature of the game to be effective at challenging their awareness. The pressure of the time limit made participants subconsciously reinforce the purpose the signing out instead of leaving the computer open to deal with issues in the office area. While it would be faster to stay signed in, it was a security risk and could lead to a quick game over.

The response of participant 5 also shows more insight on the results from the previous question about who a cybersecurity threat can be. Being forced to remember why it is recommended that players log out every time they leave their area reinforces the idea that anybody can be a threat.

Question: "How effective was the game in rewarding correct actions and penalising incorrect actions towards maintaining data security?

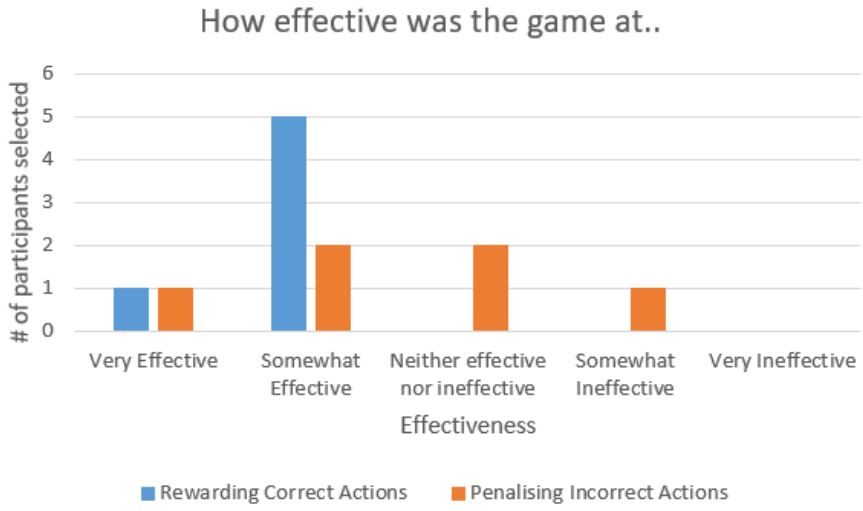

Figure 55 - Reward/Penalty Effectiveness Bar Chart

The positive and negative feedback loop of an educational game is an important aspect to the teaching experience. Evidently, the negative feedback portion of the game was not seen as effective by a convincing enough margin. The negative feedback loop was limited to losing points, and/or losing the level, which does not inform the player the way they would be in a real scenario of having your data breached. In that aspect, the game is not completely realistic to the type of experience it is trying to simulate, unlike some successful simulation games (Backlund, Hendrix 2013).

Measuring Interest

Question: "How engaging did you find the game?"

Participant Num	Engagement Rating (1 Bad - 10 Good)
Participant 1	7.00
Participant 2	7.00
Participant 3	10.00
Participant 4	5.00
Participant 5	9.00
Participant 6	8.00
AVG	**7.67**

Table 23 - Engagement Rating

As an experience, the game was very well received by participants. Despite not all participants agreeing that they learned something new from the game, all of them could agree that the game was engaging to play. The game was successful in terms of catching the player's attention, with most participants feeling strongly about it in this aspect.

Question: "What aspects of the game stood out to you?"

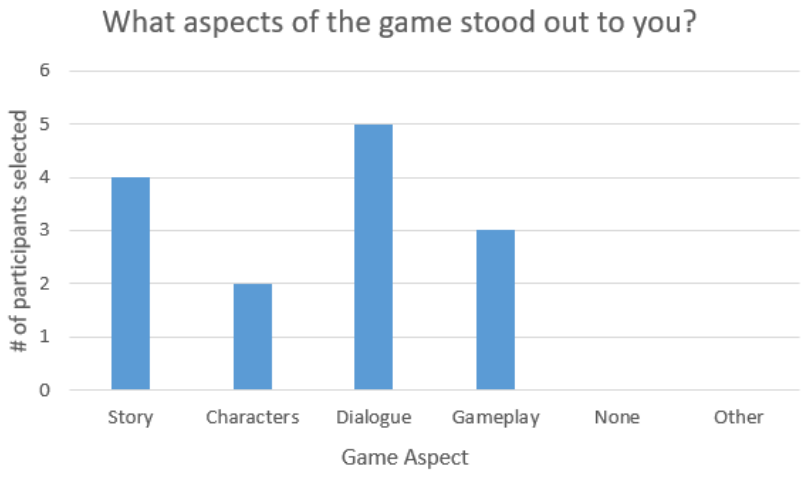

Figure 56 - Standout Aspect Bar Chart

With these results, it's now evident that the story and dialogue acted as the main point of interest regarding the game. It was also evident with how many participants believed that they had a better understanding of social engineering above all other cyber threats that the game represented. The story explained through dialogue had successfully created interest in the content, this is an integral part to knowledge retention and proper influence (Bada, Sasse and Nurse, 2019). Gameplay did not stand out as much in comparison, but it was clearly still a factor in the high engagement scores.

Question: "Do you prefer this method of learning compared to the most preferred method you chose in the previous survey?"

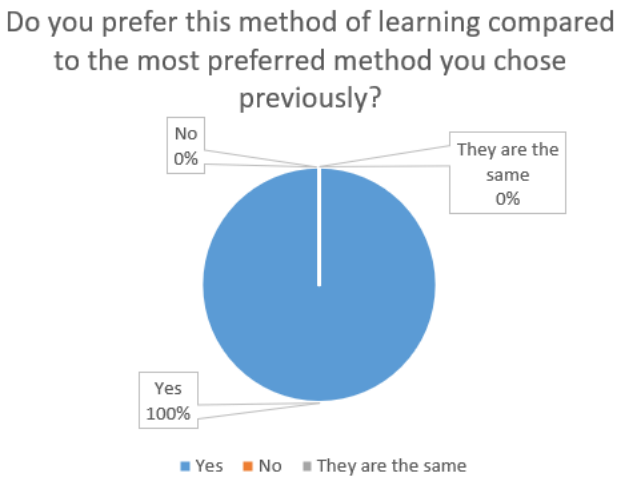

Figure 57 - Learning Method Preference Pie Chart

This is potentially the most interesting result of the survey. Despite half of the recipients not believing that their understanding of cybersecurity concepts had improved, the unanimous opinion is that they preferred the learning experience that the game provided over other methods they chose in the previous survey. This includes reading, lectures, seminars, and videos. I interpret this to be a result of the games engagement; it did not provide much new information to experienced players, but they recognised the potential value in this approaches method of teaching. The game was able to communicate information through an engaging story and gameplay that required serious focus.

Question: "In the future, assuming this game were to be expanded upon with more gameplay, more game-ified cybersecurity mechanics, more story, and more content in general, would you revisit the game?"

Participant Num	Revisit Game?	Reason
Participant 1	Yes	Learning
Participant 2	Yes	Entertainment
Participant 3	Yes	Entertainment
Participant 4	Yes	Learning
Participant 5	Yes	Entertainment
Participant 6	Yes	Learning

Table 24 - Revisit Game

These results further prove that the game has been recognised for its potential as both entertainment and a learning tool. It is noteworthy that the lesser experienced participants

favoured the idea of returning to learn, while participants that expressed more confidence in the topic pre-gameplay favoured entertainment. This could possibly imply that experienced players do not value the educational aspects, and see it as entertainment? Although, these participants already expressed interest in the educational aspect in the previous question.

Question: "How much would you be willing to commit to access this theoretical extended game?"

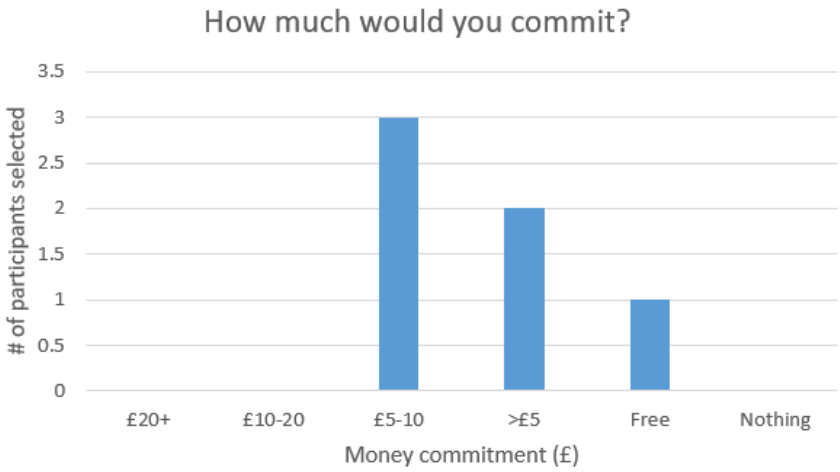

Figure 58 - Money Commitment Bar Chart

This question was used to measure the level of commitment that participants had to revisiting the game. The consensus was a price under £10. While this is far from the pricing of commercial games released on consoles, it is more in line with games sold by individual developers on online video game store platforms, such as steam.

7.3 Summary

My findings from these results highlighted some strengths and weaknesses of my solution. While traditional cybersecurity training provides a foundation, an engaging, game-based approach can significantly enhance confidence and interest in cybersecurity. The game did not have an equal impact on all participants, results imply that the game as an educational experience has been tailored more to those with less knowledge, partially leaving more experienced participants out. The game is inferior to training and courses in that aspect. However, experienced participants were still able to gain more confidence in recognising certain threats like social engineering and phishing scams, due to how they were tied into an engaging story and gameplay that reinforced learning.

Participants could recognise each cyber threat, as each participant was able to highlight at least one area they improved in. The game's ability to present information through an engaging

narrative and interactive gameplay proved effective in capturing attention and potentially facilitating better knowledge retention. This suggests that expanding the game could further capitalize on its strengths as an educational tool, appealing to both novices and those with prior cybersecurity experience.

8 Conclusions

1. “Incorporate several cyber security concepts that cover the most common cyber-attacks within gameplay, to cover the most vital cybersecurity information.”

I directly used different cyber threats such as phishing, social engineering, insider threats, spoofing and man-in-the-middle attacks as inspiration for game mechanics and story plot points during both the design and implementation phases. These concepts were deemed to be the most relevant to the current state of cybersecurity through research and reviews of background literature.

2. “Design and implement unique game mechanics for the different cyber threats and common errors that lead to breaches, to make each threat stand out.”

Participants that played the game were able to identify the previously listed concepts during gameplay and believed that the game improved their ability to recognise the cyber threats that these mechanics represented.

3. “Represent threats to a user’s cybersecurity both inside and outside of the digital landscape to encourage a change of cybersecurity habits rather than only threat recognition.”

The game uses both story and gameplay to influence players. The story took the main role of explaining, representing and portraying threats outside of the digital landscape such as potential bad actors and insider threats that can exist in workplaces. The game received the most praise for this aspect by participants from the post-game survey, and their improved answers to the question of “who do you think poses a threat to cybersecurity” further supports the fact that these threats outside of the landscape were recognised. Threats inside the landscape were represented by the main gameplay loop of answering emails and trying to decipher their intent.

4. “Create mechanics that can act as a form of cybersecurity “training” for both experienced and un-experienced players.”

While the game was better received by those less experienced in cybersecurity, the game was still found as beneficial to those with experience in cybersecurity. Every participant, regardless

of background, preferred the games method of teaching and training compared to reading, watching videos, or listening to lectures and seminars. The game was valued for its gameplay capabilities, and conditioning players to constantly think about why they do actions such as logging out of a computer every time they leave it.

5. "Create an engaging learning experience by creating an interesting story/narrative that ties into the topic of cybersecurity."

The dialogue and story were by far the most praised aspects of the game. Engagement scores were high, and half of all participants grew genuine interest at the prospect of a completed version of the game based on its entertainment merits.

Even though I believe I achieved all objectives to a satisfactory level, I do not see my current solution to be an improvement to the popular existing methods of raising cybersecurity awareness and informing people of how to stay safe. During research, I put too much emphasis on the failures of cybersecurity campaigns and training courses at building genuine interest in the topic, and attributing value to the information they were trying to communicate. While this led to me creating a very engaging experience, my game fell flat when it came to delivering new or in-depth information about cybersecurity and the threats that users can face. A significant change in understanding was only observable through participants that had below average cybersecurity knowledge.

It would also be naïve to think that my sample size of participants would accurately estimate the effectiveness of my solution for a problem that is the concern of over millions of individuals around the world. However, the results I have observed give me confidence that my solution could stand amongst the conventional means of raising awareness, such as campaigns, training courses, and above other educational cybersecurity games, if it were fully developed and given appropriate exposure.

8.1 Future Work

When starting this project, I was limited by my lack of experience in Unity and the C# programming language. This severely slowed down the design and implementation processes of the project, forcing me to cut planned features and shrink my scope in terms of design. This included:

- **Levels with completely randomised events and emails:** I considered the use of generative AI to randomly create emails for the email manager, so that levels could feel different even when played multiple times. I also had other planned in-game events like the broken device minigame, that would give the player different responsibilities while playing the game outside of interacting with the main cybersecurity mechanics.
- **Different stages:** I originally planned more than one main area for gameplay. For example, the player could be required to complete their work in an internet café or at home. This would have given me even more opportunity to highlight other cybersecurity concepts such as networks.
- **Penalties that affect gameplay directly:** For example, clicking on a malware link would slow the players computer down until they did a system restore; or a weak passcode for the scanner requiring the player to find the employee that stole the documents inside. These penalties would have made these cybersecurity concepts feel even more unique.
- **Database for saving progress and using past sessions to influence new ones:** A database was planned, to save the scores of players and use that data for an even better evaluation. This database would have also recognised what players struggled with the most during gameplay, and changed levels in a way that would train them according to what they struggled with.

It was likely obvious, but I had a lot of fun with creating the story elements, such as fun dialogue between characters and designing cutscenes. If it were not for the focus of this project being the informing and training aspects, I would have likely explored more of the story aspects, creating more cutscenes and characters interactions. With how well-received the game was in such an unfinished state, I have a lot of motivation to take this project even further past this dissertation.

References

[1] Fortinet Training Institute (2023) *Security Awareness and Training Global Research Brief.* Available at:
https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2023-security-awareness-and-training.pdf
(Accessed: 5 March 2024)

[2] Horowitz, M., (2023) *2023 Mid-Year Cyber Security Report.* Available at:
https://www.checkpoint.com/downloads/resources/2023-mid-year-cyber-security-report.pdf?mkt_tok=NzUwLURRSC01MjgAAAGPCtGnSn-mFLcUWkGX3Gc9_S_4aJaYJzRbSPDJMLqSh6f19kjlaEzOLmSvRDdroKnp51E9KmGEQ84JAbgRztNLYasRoTYBkzkgeMlvlcWXBuX0me1R
(Accessed: 5 March 2024)

[3] Bada, M., Sasse, A.M., and Nurse, J.R.C., (2019) *Cyber Security Awareness Campaigns: Why do they fail to change behaviour? ArXiv*, [online] Available at:
https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf
(Accessed: 5 March 2024)

[4] Alotaibi, F., Furnell, S., Stengel, I., and Papadaki, M., (2016) *A Review of Using Gaming Technology for Cyber-Security Awareness. International Journal for Information Security Research (IJISR)*, [online]. Available at:
https://infonomics-society.org/wp-content/uploads/ijisr/published-papers/volume-6-2016/A-Review-of-Using-Gaming-Technology-for-Cyber-Security-Awareness.pdf
(Accessed: 5 March 2024)

[5] National Cybersecurity Alliance, (2022) *About Cybersecurity Awareness Month* [online] Available at:
https://staysafeonline.org/programs/about-cybersecurity-awareness-month/
(Accessed: 20 March 2024)

[6] NHS England, (2023) *Cyber Security Awareness Month 2023* [online] Available at:
https://digital.nhs.uk/cyber-and-data-security/campaigns/cyber-security-awareness-month-october-2023#top
(Accessed: 20 March 2024)

[7] Kate, R. (2023) *The logic behind three random words* [online] Available at: https://www.ncsc.gov.uk/blog-post/the-logic-behind-three-random-words (Accessed: 20 March 2024)

[8] Puzder D. (2022) *Cybersecurity Awareness Month: Updates* [online] Available at: https://informationsecurity.wustl.edu/cybersecurity-awareness-month-phishing-2-2-2/ (Accessed: 20 March 2024)

[9] Smith, D.T. and Ali, A.I., (2019). *You've Been Hacked: A Technique for Raising Cyber Security Awareness. Issues in Information Systems, 20(1),* pp.186-194 [online] Available at: https://iacis.org/iis/2019/1_iis_2019_186-194.pdf (Accessed: 20 March 2024)

[10] Lindsey, R.V., Shroyer, J.D., Pashler, H., and Mozer, M.C., (2014). *Improving Students' Long-Term Knowledge Retention Through Personalized Review. Psychological Science, 25(3),* pp.639–647. [online]. Available at: https://journals.sagepub.com/doi/full/10.1177/0956797613504302#bibr10-0956797613504302 (Accessed: 20 March 2024)

[11] Peña-Miguel, N. and Sedano Hoyuelos, M., (2014). *Educational Games for Learning. Universal Journal of Educational Research, 2(3),* pp.230-238. [online]. Available at: https://eric.ed.gov/?id=EJ1053979 (Accessed: 20 March 2024)

[12] Zeng, J., Parks, S., and Shang, J., (2020). To learn scientifically, effectively, and enjoyably: A review of educational games. *Human Behavior and Emerging Technologies*, 2, pp.186–195. https://onlinelibrary.wiley.com/doi/epdf/10.1002/hbe2.188 (Accessed: 20 March 2024)

[13] Backlund, P. and Hendrix, M., (2013). *Educational Games – Are They Worth The Effort? A Literature Survey of the Effectiveness of Serious Games*. *International Journal of Serious Games*, [online] Available at: https://ieeexplore.ieee.org/abstract/document/6624226 (Accessed: 20 March 2024)

[14] Antonova, A., Bontchev, B. (2019) *EXPLORING PUZZLE-BASED LEARNING FOR BUILDING EFFECTIVE AND MOTIVATIONAL MAZE VIDEO GAMES FOR EDUCATION, EDULEARN19 Proceedings*, pp. 2425-2434. [online] Available at:

https://library.iated.org/view/ANTONOVA2019EXP

(Accessed: 20 March 2024)

[15] Hendrix, M, Al-Sherbaz, A & Victoria, B (2016), 'Game based cyber security training: are serious games suitable for cyber security training?', *International Journal of Serious Games*, vol. 3, no. 1, pp. 53-61. [online] Available at:

https://doi.org/10.17083/ijsg.v3i1.107

(Accessed: 20 March 2024)

[16] Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., and Briggs, P., (2022). Exploring Age and Gender Differences in ICT Cybersecurity Behaviour. *Human Behavior and Emerging Technologies*, [online] Volume 2022, Article ID 2693080. Available at:

https://doi.org/10.1155/2022/2693080

(Accessed: 20 March 2024)

[17] Le Compte, A., Elizondo, D., and Watson, T., (2015). A Renewed Approach to Serious Games for Cyber Security. *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, [online] Available at:

https://ieeexplore.ieee.org/abstract/document/7158478

(Accessed: 20 March 2024)

[18] Nitz, J. C., Kuys, S., Isles, R. and Fu, S., (2010) *Is the Wii Fit™ a new-generation tool for improving balance, health and well-being? A pilot study, Climacteric*, 13:5, 487-491, [online]. Available at:

https://www.tandfonline.com/doi/full/10.3109/13697130903395193

(Accessed: 20 March 2024)

[19] Müller, A., (2017). *Undertale: Violence in Context. [pdf] Simon Fraser University*. [online] Available at:

https://summit.sfu.ca/_flysystem/fedora/sfu_migrate/17572/etd10369_AM%C3%BCller.pdf

(Accessed: 20 March 2024)

[20] Milne, C. (2024). *Video Game Narrative: The Different Types and How-to Start Writing; pinnguaq.* [online] Available at:

https://pinnguaq.com/learn/video-game-narrative/

(Accessed: 20 March 2024)

[21] Welsh, E.M., (2017). *How to Write a Good Video Game Story; emwelsh* [online]. Available at:

https://www.emwelsh.com/blog/write-good-video-game-story

(Accessed: 20 March 2024)

[22] Brazie, A., (2024). *Designing the Core Gameplay Loop: A Beginner's Guide; gamedesignskills* [online]. Available At:

https://gamedesignskills.com/game-design/core-loops-in-gameplay/#what-is-a-gameplay-loop

(Accessed: 20 March 2024)

Appendix A Personal Reflection

A.1 Reflection on Project

The nature of this project makes objective statistical analysis difficult. Enjoyment of a product is completely up to the interpretation of the player, meaning that a large part of this game was always going to hinge on the subjective opinions of others. Even if I had a sample size of 100 people to play the game, and received overwhelmingly positive results, there is no guarantee that those results would translate to success amongst a larger audience.

I underestimated the amount of work that game development takes. As the deadline of the project came closer, I was forced to cut a significant number of planned features. I realised halfway into the development process that the full scope of my project was impossible within the given timeframe.

I used generative AI during the design process to help me think of some ideas for game mechanics based on the research I did. I took some of the ideas ChatGPT came up with and changed them to my liking. ChatGPT was also used during the implementation process to help me fix errors in Unity that I could not find or understand. Due to my lack of knowledge of C# before this project, ChatGPT was also used at the start of implementation to show me how to write certain basic programming terminology in C#. Generative AI helped speed up the implementation process by filling my knowledge gaps in Unity and C# until I understood the tools enough to do everything I wanted to.

A.2 Personal Reflection

Given my time again, I would have focused more on what work was feasible in the given timeframe. I also would have left less of the dissertation write-up for the end of the project and written more sections of it as the program was developed. I would have also looked for participants earlier into the project to have more of them and guarantee their participation.

Appendix B Ethics Documentation

B.1 Ethics Confirmation

College of Engineering, Design and Physical Sciences Research Ethics Committee
Brunel University London
Kingston Lane
Uxbridge
UB8 3PH
United Kingdom

www.brunel.ac.uk

21 December 2023

LETTER OF APPROVAL

APPROVAL HAS BEEN GRANTED FOR THIS STUDY TO BE CARRIED OUT BETWEEN 01/02/2024 AND 22/03/2024

Applicant (s): Mr Tolu Olasupo

Project Title: Creating Engaging, Timeless Cybersecurity Awareness

Reference: 46705-LR-Dec/2023- 48794-1

Dear Mr Tolu Olasupo

The Research Ethics Committee has considered the above application recently submitted by you.

The Chair, acting under delegated authority has agreed that there is no objection on ethical grounds to the proposed study. Approval is given on the understanding that the conditions of approval set out below are followed:

- **The agreed protocol must be followed. Any changes to the protocol will require prior approval from the Committee by way of an application for an amendment.**
- **Please ensure that you monitor and adhere to all up-to-date local and national Government health advice for the duration of your project.**
- **Please remove your personal email address from your Participant Information Sheet and replace it with your Brunel one**
- **Please add the following into your Participant Information Sheet 1) your Brunel email address 2) your supervisor's name and email address 3) a line at the end to state that for queries and complaints, your participants may contact Professor Simon Taylor (simon.taylor@brunel.ac.uk) – Chair of the CEDPS Research Ethics Committee**

Above points can be addressed outside of the BREO system.

Please note that:

- Research Participant Information Sheets and (where relevant) flyers, posters, and consent forms should include a clear statement that research ethics approval has been obtained from the relevant Research Ethics Committee.
- The Research Participant Information Sheets should include a clear statement that queries should be directed, in the first instance, to the Supervisor (where relevant), or the researcher. Complaints, on the other hand, should be directed, in the first instance, to the Chair of the relevant Research Ethics Committee.
- Approval to proceed with the study is granted subject to any conditions that may appear above.
- The Research Ethics Committee reserves the right to sample and review documentation, including raw data, relevant to the study.
- If your project has been approved to run for a duration longer than 12 months, you will be required to submit an annual progress report to the Research Ethics Committee. You will be contacted about submission of this report before it becomes due.
- You may not undertake any research activity if you are not a registered student of Brunel University or if you cease to become registered, including abeyance or temporary withdrawal. As a deregistered student you would not be insured to undertake research activity. Research activity includes the recruitment of participants, undertaking consent procedures and collection of data. Breach of this requirement constitutes research misconduct and is a disciplinary offence.

Professor Simon Taylor

Chair of the College of Engineering, Design and Physical Sciences Research Ethics Committee

Page 1 of 2

Appendix C Other Appendices

More relevant material

C.1 Story related maps

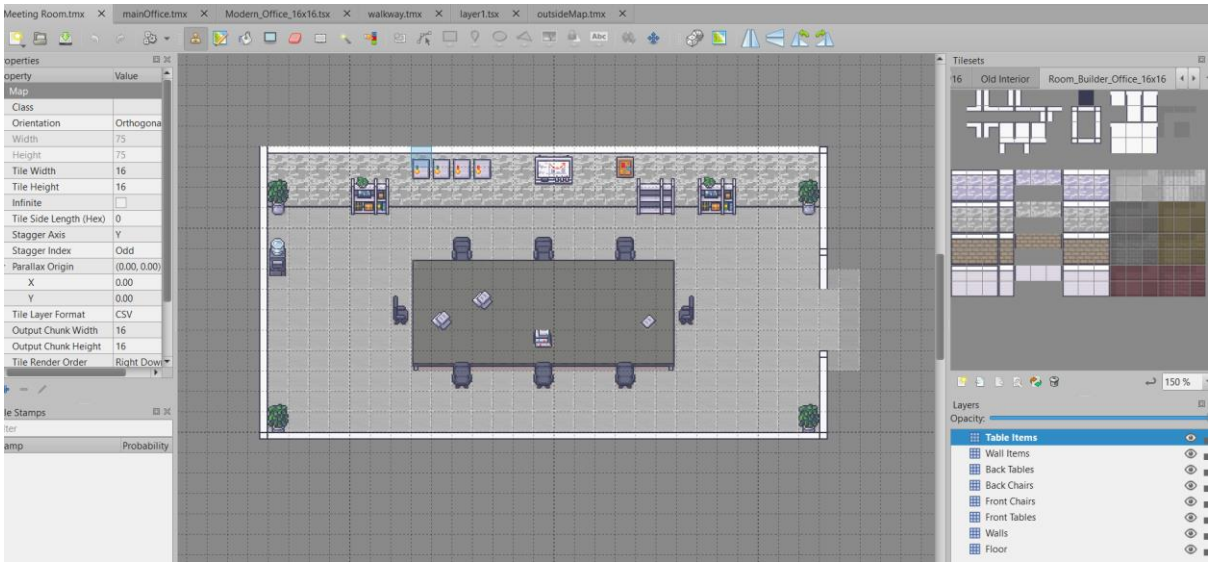

Figure 59 - The Meeting Room in tiled

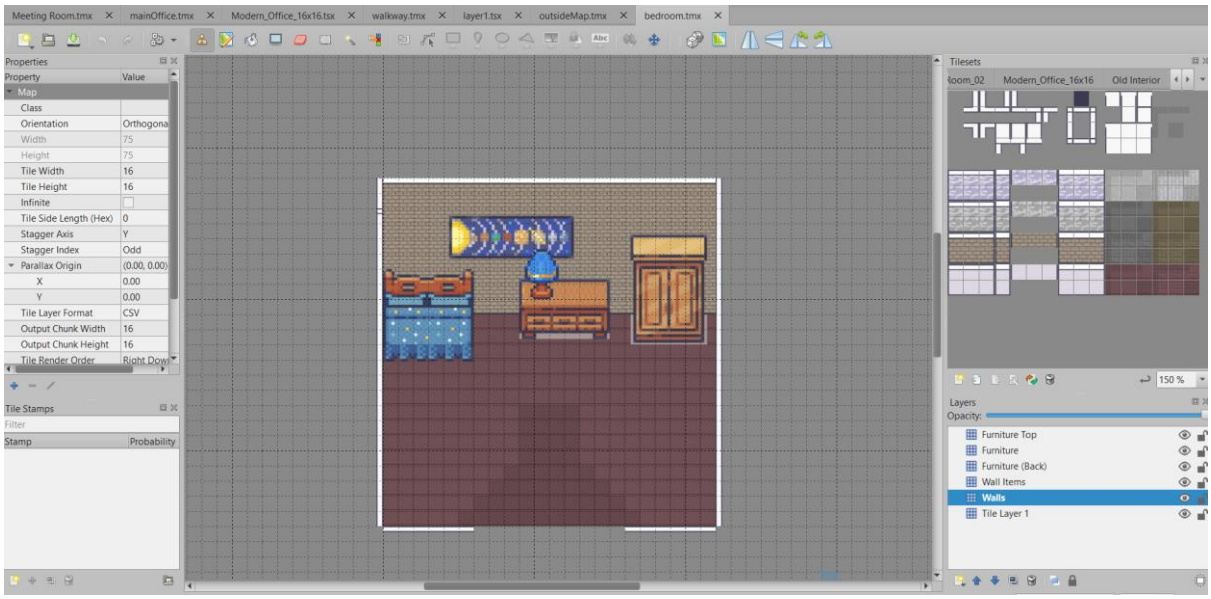

Figure 60 - Player Bedroom in tiled

Figure 61 - Dialogue Example 1

Figure 62 - Dialogue Example 2

Figure 63 - Dialogue Example 3

Figure 64 - Dialogue Example 4

Figure 65 - Dialogue Example 5

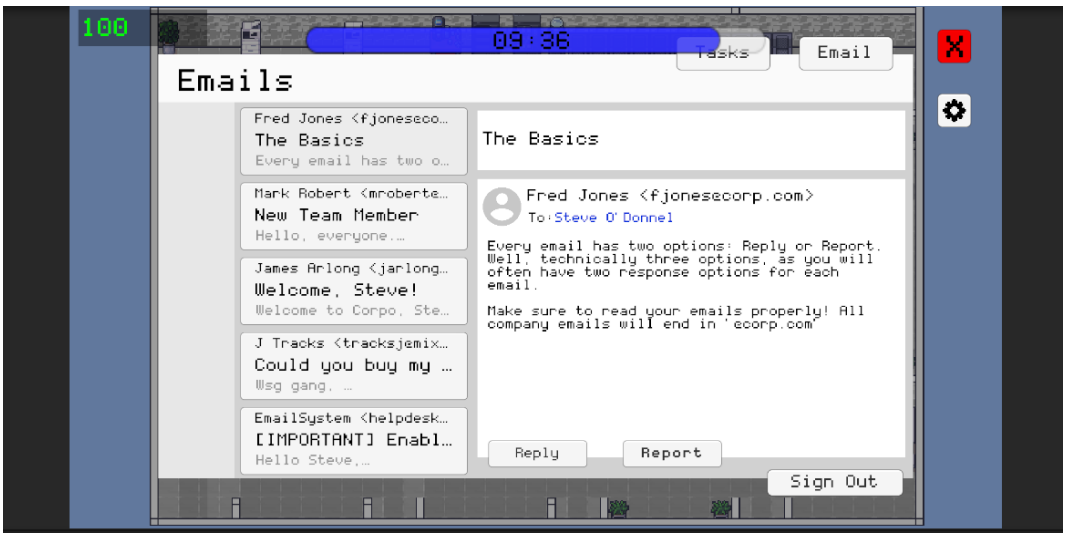

Figure 66 - Email Screen Example

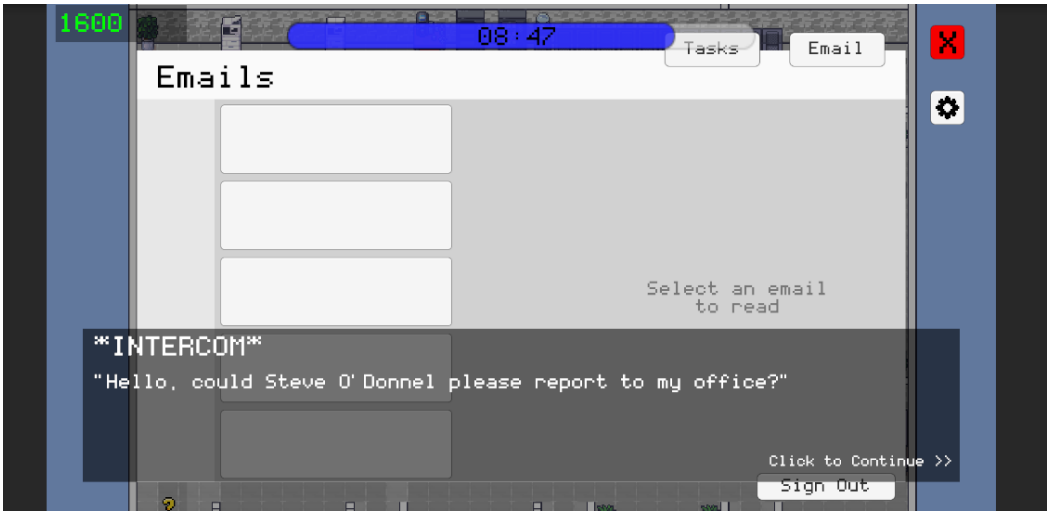

Figure 67 - Player Completes Level Example

Figure 68 - Dialogue Example 6

Figure 69 - Dialogue Example 7

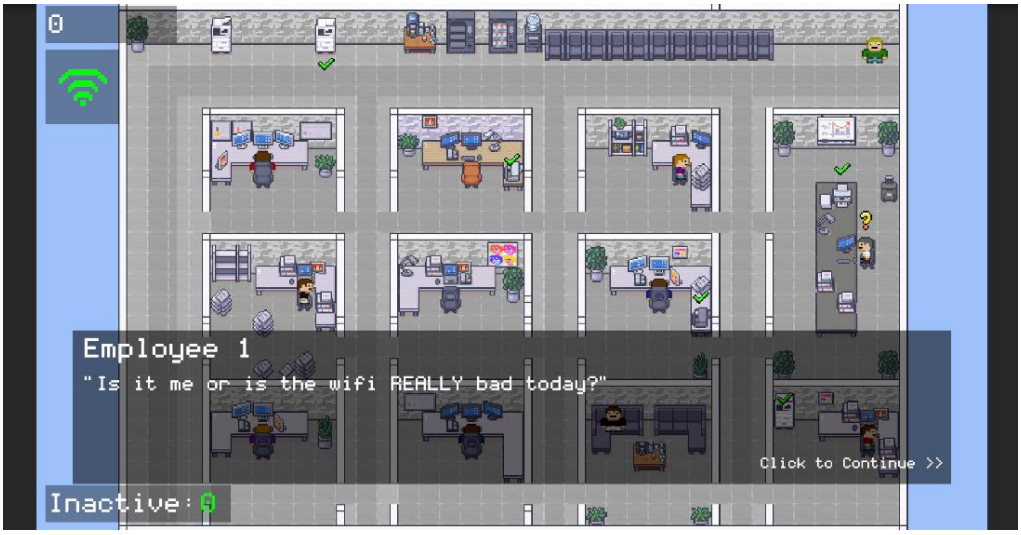

Figure 70 - Dialogue Example 8

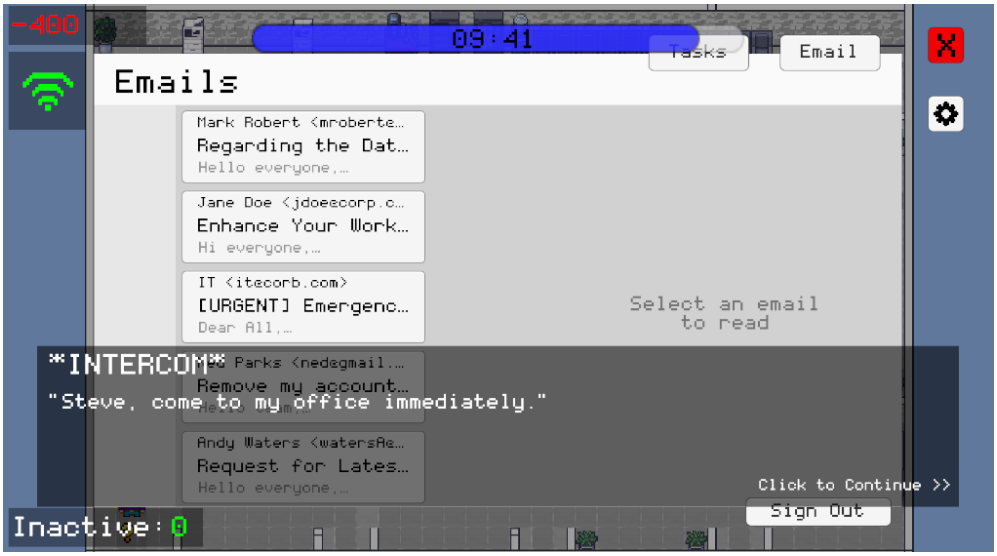

Figure 71 - Level Failure Example

Figure 72 - Level Failure Example 2