Research Document

Cybersecurity Educational Training Videogame

Peter Hyland – C000274825

Abstract

Cybersecurity awareness and training is a critical challenge for many companies around the world. Despite many companies prioritising Cybersecurity training and awareness, many still are lacking in their approach to training their employees. This in turn leads to employees falling victim to Cybersecurity threats such as phishing e-mails and improper Cyber hygiene. As part of my research, I intend to highlight how the gamification of Cybersecurity training through the medium of a video game can enhance typical cyber security training, adding an engaging aspect to it and instilling a strong cyber security culture in these organisations.

Through the medium of a videogame, possibly either the Unity game engine or the Unreal game engine, I intend to an escape room-style game, this project intends to create an immersive and engaging learning experience that educates employees on common security vulnerabilities, such as phishing attacks, password security, social engineering, and emerging threats. By leveraging the principles of gamification, the game seeks to improve knowledge retention, promote practical application of cybersecurity concepts, and foster a proactive security mindset among participants.

This research will analyse the effectiveness of gamified training approaches, drawing insights from current examples of other games. The research will also investigate the design and gameplay elements and how best to create an engaging and educational experience; while also outlining some challenges I may encounter as a solo game developer with no prior game development experience.

Table of Contents

Introduction

Cybersecurity is a rapidly evolving field. Familiarising yourself with evolving threats and getting a refresher on existing current threats which threat actors utilise is crucial for any organisation. Through the gamification of Cybersecurity, I intend to improve retention on employees. A recent Stanford Research study (Knowbe4, n.d.)showed that a significant 88% of data breaches are caused by human error. By engaging employees and the public on the importance of good cyber hygiene and best practices I hope to instil better cybersecurity posture for organizations which use my video game for training.

Training of employees proper Cybersecurity principles and concepts is vital. However, despite the growing importance of cybersecurity, many organizations in the European Union are falling short in terms of training and awareness. A recent Eurobarometer survey revealed that although 71% of companies recognize cybersecurity as a high priority, a surprising 74% have not conducted any training or awareness programs for their employees (Eurobarometer, 2024) The survey also found that 68% of companies believe no training is needed, with 16% unaware of training opportunities and 8% citing budget constraints.

This lack of cybersecurity training and awareness is particularly concerning given the increasing frequency and sophistication of cyber threats. As highlighted in a recent foresight report by the EU Agency for Cybersecurity (ENISA). (ENISA, 2024) The growing cyber skills gap is a significant factor contributing to these threats, posing major risks to the operation of network and information systems and the overall integrity of the Single Market. (Eurobarometer, 2024) The ENISA also points out that “Organizations and policymakers are encouraged to adopt proactive cybersecurity measures to fortify their cybersecurity posture.” And my hope is through this videogame companies will take proactive measures and encourage their employees to take part in such interactive training. (ENISA, 2024)

To address this pressing issue, I propose the development of an educational video game that utilizes the concept of gamification to improve employee retention of cybersecurity best practices. By engaging employees and the public through an immersive, interactive learning experience, the game aims to instil better cyber hygiene habits and enhance overall cybersecurity awareness.

Via utilisation of a Unity Escape-Room style game, my educational videogame I intend to offer a low-cost solution to employers to utilize in order to further the cyber education of employees in their organization and to improve their overall cybersecurity posture.

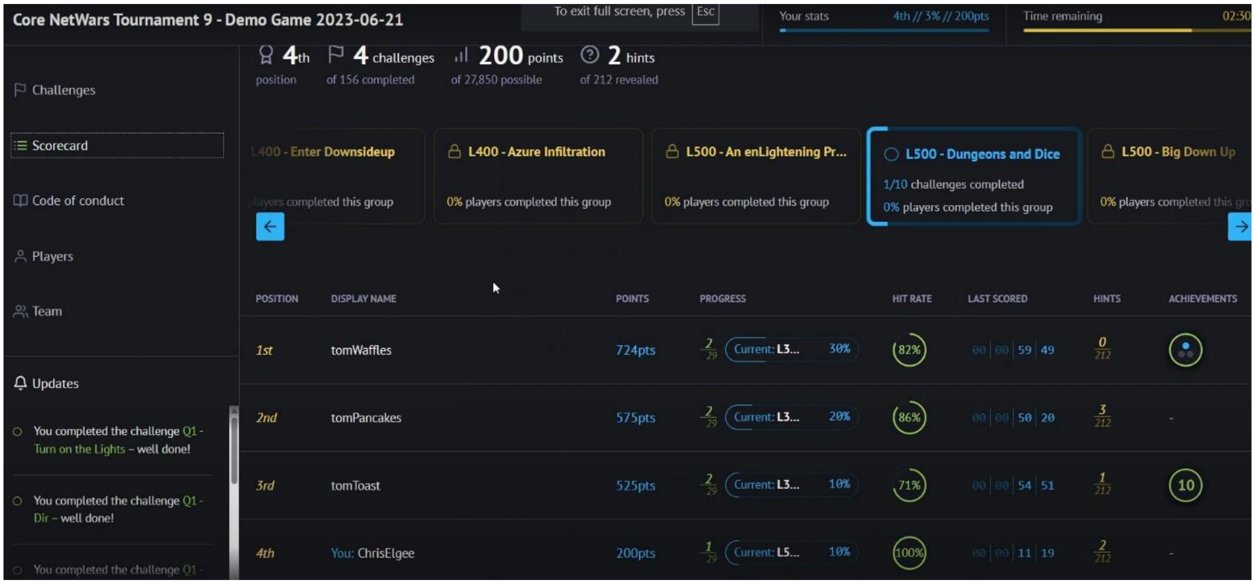
Gamification of Cyber Security Training

The integration of gamification techniques into cybersecurity training programs offers a promising approach to enhance engagement, knowledge retention, and practical application of cybersecurity concepts.

Examples

CYBRScore – Sans Institute

Existing examples, such as the "CYBRScore" platform developed by the SANS Institute, a paid training platform, have demonstrated the potential of gamified training by incorporating elements like scoring systems, leaderboards, and interactive challenges. Below is a screenshot of aforementioned CYBRScore netwars platform. (cisecurity, n.d.)



4th position · 4 challenges of 156 completed · 200 points of 27,850 possible · 2 hints of 212 revealed

L400 - Enter Downsideup — players completed this group

L400 - Azure Infiltration — 0% players completed this group

L500 - An enLightening Pr... — 0% players completed this group

L500 - Dungeons and Dice — 1/10 challenges completed — 0% players completed this group

L500 - Big Down Up — 0% players completed this gr

POSITION	DISPLAY NAME	POINTS	PROGRESS	HIT RATE	LAST SCORED	HINTS	ACHIEVEMENTS
1st	tomWaffles	724pts	2/29 Current: L3... 30%	82%	00 | 00 | 59 | 49	0/212	●
2nd	tomPancakes	575pts	2/29 Current: L3... 20%	86%	00 | 00 | 50 | 20	3/212	-
3rd	tomToast	525pts	2/29 Current: L3... 10%	71%	00 | 00 | 54 | 51	1/212	10
4th	You: ChrisElgee	200pts	1/29 Current: L5... 10%	100%	00 | 00 | 11 | 19	2/212	-

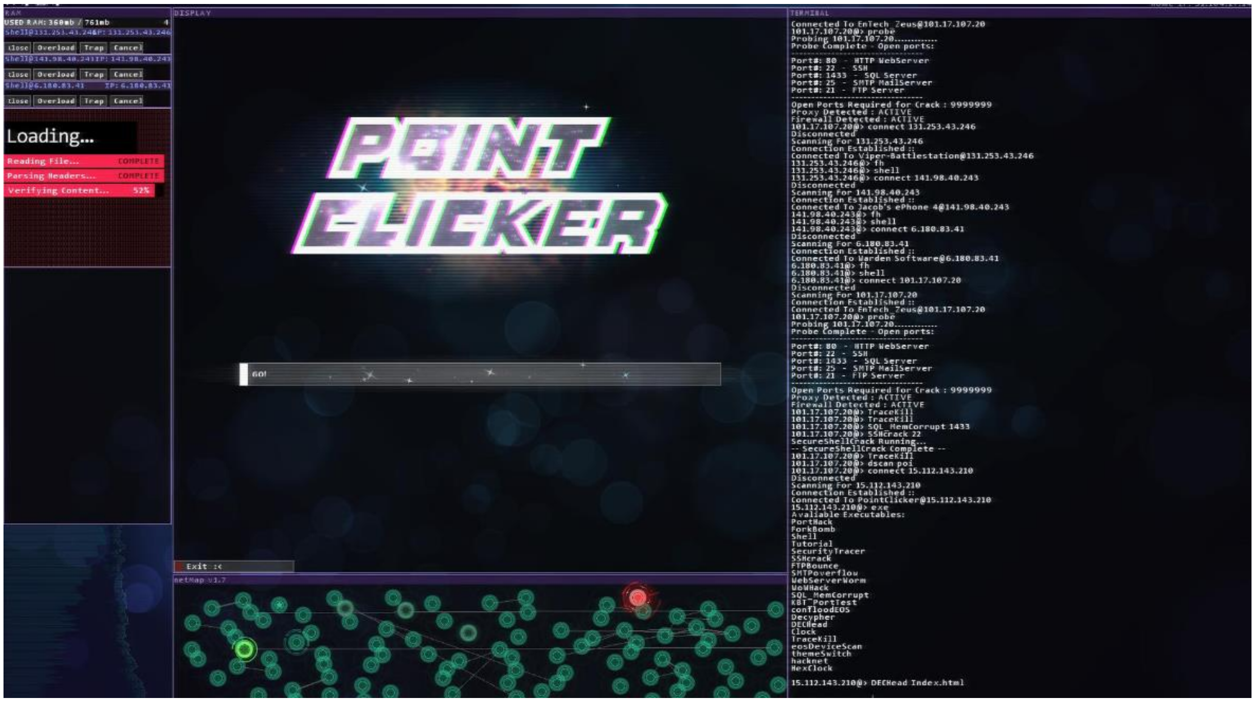
○ You completed the challenge Q1 - Turn on the Lights – well done!

○ You completed the challenge Q1 - Dir – well done!

○ You completed the challenge Q1 -

Hacknet

Another such game I analysed was https://store.steampowered.com/app/365450/Hacknet/
This is a game which follows the story of a recenltly deceased hacker. It encourages and trains you to use linux commands and active hack into things. This is more offensive security geared and not particularly the avenue I want to pursue, my area of training is primarily focused on employees and not prospective hackers.

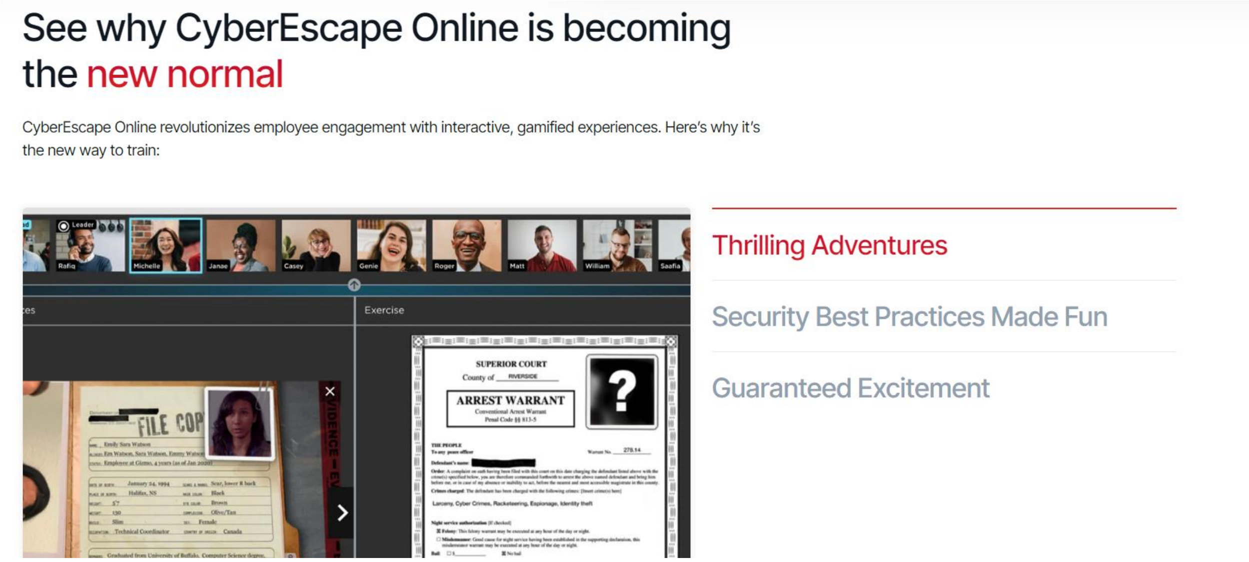


```
Connected To EnTech_Zeus@101.17.107.20
101.17.107.20@> probe
Probing 101.17.107.20............
Probe Complete - Open ports:
--------------------------------
Port#: 80  - HTTP WebServer
Port#: 22  - SSH
Port#: 1433  - SQL Server
Port#: 25  - SMTP MailServer
Port#: 21  - FTP Server
--------------------------------
Open Ports Required for Crack : 9999999
Proxy Detected : ACTIVE
Firewall Detected : ACTIVE
101.17.107.20@> connect 131.253.43.246
Disconnected
Scanning For 131.253.43.246
Connection Established ::
Connected To Viper-Battlestation@131.253.43.246
131.253.43.246@> fh
131.253.43.246@> shell
131.253.43.246@> connect 141.98.40.243
Disconnected
Scanning For 141.98.40.243
Connection Established ::
Connected To Jacob's ePhone 4@141.98.40.243
141.98.40.243@> fh
141.98.40.243@> shell
141.98.40.243@> connect 6.180.83.41
Disconnected
Scanning For 6.180.83.41
Connection Established ::
Connected To Warden Software@6.180.83.41
6.180.83.41@> fh
6.180.83.41@> shell
6.180.83.41@> connect 101.17.107.20
Disconnected
Scanning For 101.17.107.20
Connection Established ::
Connected To EnTech_Zeus@101.17.107.20
101.17.107.20@> probe
Probing 101.17.107.20............
Probe Complete - Open ports:
--------------------------------
Port#: 80  - HTTP WebServer
Port#: 22  - SSH
Port#: 1433  - SQL Server
Port#: 25  - SMTP MailServer
Port#: 21  - FTP Server
--------------------------------
Open Ports Required for Crack : 9999999
Proxy Detected : ACTIVE
Firewall Detected : ACTIVE
101.17.107.20@> TraceKill
101.17.107.20@> TraceKill
101.17.107.20@> SQL_MemCorrupt 1433
101.17.107.20@> SSHcrack 22
SecureShellCrack Running...
-- SecureShellCrack Complete --
101.17.107.20@> TraceKill
101.17.107.20@> dscan poi
101.17.107.20@> connect 15.112.143.210
Disconnected
Scanning For 15.112.143.210
Connection Established ::
Connected To PointClicker@15.112.143.210
15.112.143.210@> exe
Avaliable Executables:
PortHack
ForkBomb
Shell
Tutorial
SecurityTracer
SSHcrack
FTPBounce
SMTPoverflow
WebServerWorm
WoWHack
SQL_MemCorrupt
KBT_PortTest
confloodEOS
Decypher
DECHead
Clock
TraceKill
eosDeviceScan
themeSwitch
hacknet
HexClock

15.112.143.210@> DECHead Index.html
```

CyberEscape Online – Living Security

Living Security proudly states that it's Cyber escape room game "CyberEscape Online revolutionizes employee engagement with interactive, gamified experiences. Here's why it's the new way to train:" https://www.livingsecurity.com/products/cybersecurity-escape-games



See why CyberEscape Online is becoming the new normal

CyberEscape Online revolutionizes employee engagement with interactive, gamified experiences. Here's why it's the new way to train:

Thrilling Adventures

Security Best Practices Made Fun

Guaranteed Excitement

National Cryptologic

The National Cryptologic provides a web based unity game. I found this game engaging and was impressed by it’s web based integration using WebGL.

https://cryptologicfoundation.org/students/games/original-game.html

CyberCIEGE

https://nps.edu/web/c3o/cyberciege

Another notable example is "CyberCIEGE," an interactive simulation developed by the Naval Postgraduate School that immerses players in the role of a decision-maker tasked with managing the cybersecurity of a fictional organization. While highly realistic and comprehensive, its complexity may intimidate non-technical users.

Gamification

A research study titledstudy on “Gamification Techniques for Raising Cyber
Security Awareness” had some interesting insights into Gamification for raising Cyber security awareness..
(Scholefield, n.d.)

Gamification can be defined as "the application of gaming mechanics to non-gaming contexts with the aim of inducing engagement and raising levels of motivation" (Growth Engineering, 2018, as cited in Scholefield & Shepherd, 2019, p. 2).

A study by Domínguez et al. (2013) found that while students who engaged with gamified content performed poorly on written tasks, they performed strongly on practical tasks, suggesting that gamification may be effective when used in the right context (as cited in Scholefield & Shepherd, 2019, p. 8).

The use of fantasy contexts, such as scenarios involving pirates and detectives, can motivate children to learn, as demonstrated by Parker and Lepper (1992) in their study on the Logo programming language (as cited in Scholefield & Shepherd, 2019, p. 9).

Providing feedback is crucial when utilizing gamification, particularly in an educational setting, as it prevents confusion about the current task (Ibanez, Di-Serio, & Delgado-Kloos, 2014, as cited in Scholefield & Shepherd, 2019, p. 8).

The study conducted by Scholefield and Shepherd (2019) found that participants enjoyed playing the RPG-style password security awareness application and felt that gamification was a useful method for raising security awareness (p. 7).

For my own videogame I feel that attempting to educate people through the use of the medium of this videogame will prove very useful.

Design and Gameplay

I intend for the gameplay to explore a wide variety of Cybersecurity concepts to reinforce the employees' learning. Including but not limited to:

Social Engineering

Employees will encounter simulated social engineering attacks, such as pretexting, phishing, and baiting, where they must identify and respond appropriately to these deceptive tactics.

According to 2022 – State of Cybersecurity report (icasa.org, n.d.) Social engineering is a leading for breaches of company data. I intend to create an in-game scenario where the player receives a phone call from someone claiming to be from the IT department, asking for their login credentials. The player must choose the appropriate response, such as verifying the caller's identity through official channels or reporting the incident to the actual IT department.

Phishing E-mails

The gameplay will incorporate phishing e-mails, recognizing and mitigating phishing attempts will be a central focus. Employees will analyse suspicious emails, scrutinize URLs, attachments, and embedded content, learning to differentiate legitimate communications from malicious ones.

Within the gameplay there will the player must spot the differences between a legitimate email and a phishing email, highlighting key indicators such as the sender's email address, spelling and grammar errors, or suspicious URLs

Leaving sensitive information online

The game will have a scenario which will highlight the risks of inadvertently exposing sensitive data, whether through online oversharing, improper disposal of confidential documents, or lack of physical security measures.

I intend to design a scenario where the player's character inadvertently shares sensitive company information on social media. The player must take steps to mitigate the damage, such as deleting the post, reporting the incident, and following the company's data breach response plan.

Password Security

Employees will learn the importance of strong, unique passwords and the dangers of password reuse and weak credentials. They will practice creating and managing secure passwords while defending against common password-cracking techniques.

I intend to simulate a password-cracking attempt within the game, where the player must defend against various techniques like brute-force attacks or dictionary attacks by implementing strong password policies and multi-factor authentication.

Insider Threats

IBM classifies Insider threats as “Insider threats are cybersecurity threats that originate with authorized users, such as employees, contractors and business partners, who intentionally or accidentally misuse their legitimate access, or have their accounts hijacked by cybercriminals.” (ibm.com, n.d.)

The game will explore the potential risks posed by malicious insiders, such as disgruntled employees or those susceptible to bribery or coercion. Employees will learn to identify and report suspicious behaviour, as well as implementing preventative measures.

Emerging threats

To stay ahead of evolving cyber threats, the game will incorporate scenarios involving advanced persistent threats (APTs), sophisticated phishing campaigns leveraging AI-generated content, and emerging attack vectors like deepfakes or AI-powered social engineering. As technology advances, cybercriminals are adopting new techniques to evade detection and increase the effectiveness of their attacks. For example, deepfakes, which use AI to create convincing fake videos or images, are becoming a growing concern for social engineering and disinformation campaigns. (europol, n.d.) By exposing employees to these emerging threats, the game aims to build their resilience and adaptability in the face of an ever-changing threat landscape.

Physical security

Employees will confront scenarios that test their awareness of physical security measures, such as tailgating, access control (leaving laptops in their car exposed), and secure disposal of sensitive materials.

One of the levels will have the player who must properly dispose of virtual confidential documents by dragging them to the correct bin (e.g., shredder or secure disposal) while avoiding public trash cans or recycling bins.

I also intend to design a virtual office environment where the player must identify and address physical security risks, such as ensuring doors are locked, properly storing sensitive documents, and preventing tailgating by unauthorized individuals.

Malware and Viruses

The game will simulate malware infections, ransomware attacks, and other malicious software threats, teaching employees how to recognize the signs and take appropriate action to contain and mitigate the damage.

I intend to incorporate a ransomware attack where the player's virtual device becomes infected. The player must follow the appropriate steps, such as disconnecting from the network, reporting the incident, and working with the IT department to restore from a backup.

Ability to pick and choose different levels

My intention is for each of these game elements will be separate to each other. So if an employee wishes to explore one topic and not the other, they can freely select it from the menu. Alternatively, they are free to play the game from start to finish to explore all areas of the game.

This flexibility caters to different learning preferences and time constraints, ensuring that employees can focus on the areas most relevant to their roles and responsibilities. By providing a customizable learning experience, the game aims to maximize engagement and knowledge retention.

Engaging story

I intend to have engaging gameplay with an integrated story. The employee for example done a mistake, click on a phishing e-mail and is brought through a journey of education and exploration of key concepts.

Gameplay

The cybersecurity training game will primarily be designed as an escape room-style puzzle game, where players must solve a series of challenges and puzzles to progress through the story and unlock new levels. This genre is well-suited for presenting cybersecurity concepts in an engaging and interactive manner, as it encourages critical thinking, problem-solving, and decision-making skills. However, I also intend to incorporate other genre of videogames such as specs of RPG games with dialogue and action elements with mini “boss challenges” and perhaps some elements of shooting games or similar.

Environmental Puzzles: The game will feature a variety of puzzles embedded in the virtual environment, such as decoding encrypted messages, finding hidden clues in a virtual office, or navigating through a secure network by solving network topology challenges. These puzzles encourage exploration and attention to detail.

Cybersecurity Challenges: Players will encounter challenges that directly test their understanding of cybersecurity concepts, such as configuring firewalls, identifying phishing emails, or setting up multi-factor authentication. These challenges are designed to reinforce best practices and provide hands-on experience.

As players progress through the game, they will encounter increasingly complex challenges that build upon the concepts and skills acquired in earlier levels. This scaffolded learning approach ensures that players are continually challenged and motivated to improve their cybersecurity competencies. The game's narrative structure, combined with the diverse gameplay elements, creates an immersive and memorable learning experience that effectively reinforces cybersecurity best practices and prepares employees to handle real-world threats.

Challenges

Game Development

As a novice in the realm of game development, I will face a steep learning curve in mastering the intricacies of game design, programming, and asset creation. Acquiring proficiency in the Unity game engine and its associated toolset, as well as developing a solid understanding of C# programming language, will be crucial to overcome this challenge.

As a Cyber security student, I lack any thorough knowledge of a game developments cycle nor it's inner workings. Therefore, this presents a challenge for me. However, I intend to expand my knowledge, including doing more of C# and take also take advantage of Unity's large community of free assets and plugins via the Unity store. Unity also provides extensive documentation and there exists online many tutorials on creating various aspects of a game in Unity.

I also intend to start my game development journey with simple building blocks, such as the "roll a bowl" tutorial and build upon that to flesh out my game. However initially I intend to have a barebones game and slowly build upon and integrate more advanced features.

Time management and project planning

As a solo developer, effectively managing time and prioritizing tasks will be crucial to ensure steady progress and timely completion of the project.

Asset Development

It will also be a challenge to develop assets for the Unity game. Both 2d and 3d assets. I intend to hopefully utilise applications such as GIMP to create 2d assets and perhaps Blender to modify 3d objects. I intend to make use of any open creative commons licence content I can find to integrate into the game to reduce the workload.

Balancing the game

Balancing the game's difficulty is a critical challenge that requires careful consideration. As the developer, you may have assumptions about the users' skill levels and cybersecurity knowledge, but these assumptions may prove inaccurate. If the game is too easy, players may quickly lose interest and fail to engage with the learning content. On the other hand, if the challenges are too difficult, players may become frustrated and discouraged, leading to a high dropout rate.

To strike the right balance, it is essential to conduct thorough playtesting with a diverse group of users representing the target audience. Gather feedback on the difficulty level, pacing, and clarity of the challenges. Iterate on the design based on this feedback, adjusting the complexity and providing appropriate hints and guidance where necessary. Consider implementing dynamic difficulty adjustment (DDA) mechanisms that adapt the game's challenge level based on the player's performance, ensuring a tailored experience for users with varying skill levels. Additionally, offer multiple difficulty modes or allow players to customize the challenge level to suit their preferences. By carefully balancing the game's difficulty and providing a flexible, adaptive experience, it can cater to a wide range of users and maintain engagement throughout the learning journey.

Balancing Realism and Simplicity

While the game aims to simulate realistic cybersecurity scenarios, striking the right balance between authenticity and accessibility will be a delicate task. Oversimplification may undermine the educational value, while excessive complexity could intimidate or alienate players, hindering the learning process. This is one aspect of the game's development I will have to carefully monitor.

Target audience

Target Audience Considerations

The target audience for this cybersecurity training game encompasses a diverse range of employees with varying levels of technical expertise. Striking the right balance between simplicity and depth will be essential to ensure that the game remains accessible to those with minimal technical backgrounds while still providing a challenging and informative experience for more tech-savvy individuals.

Some elements of the game will be more applicable to employees in Europe for example I may integrate some information on the new NIS2 regulations and aspects from GDPR, however these will be optional elements, I may also investigate American specific regulations to potentially incorporate.

Learn as You Play Approach

To cater to a broad audience, the game will adopt a "learn as you play" philosophy, assuming no prerequisite cybersecurity knowledge from the players. This approach necessitates a carefully crafted learning curve, gradually introducing and reinforcing concepts through gameplay mechanics, puzzles, and narrative elements. Maintaining an engaging and intuitive learning experience throughout the game will be a key challenge.

Technological Utilisation

Unity Game Engine

I will utilise the Unity game Engine. I have no prior game development experience therefore this will be somewhat of a challenge for me. I do have some programming experience, Python, Javascript and Java, however C# which is Unity's primary game engine I am not very familiar with.

Unity was chosen for its user-friendly interface and wide variety of tooling available. As a solo developer I researched which game engine to utilise such as Unreal. I found that while Unreal is a great engine it seems to be more aimed for big AAA game development big budget games. Unity suits the purpose of my game and allows for great cross platform opportunities should I wish to port my game to mobile or console and web. Alongside this Unity offers extensive documentation and active community support such as the unity developer web forum.

Beyond its core functionality, Unity offers a comprehensive suite of tools and features that will prove instrumental in crafting an immersive and engaging cybersecurity training experience. The engine's support for advanced 3D graphics, physics simulations, and audio integration will enable the creation of visually appealing and responsive environments, while its built-in animation tools will breathe life into characters and interactive elements.

Additionally, Unity's robust networking capabilities and integration with various third-party services will facilitate the implementation of multiplayer functionality, leaderboards, and online connectivity, should the need arise to incorporate these features into the training experience.

Unreal Engine is a powerful game engine known for its stunning visual capabilities and advanced features. It is widely used in the development of high-budget, AAA games and offers a robust set of tools for creating visually impressive and interactive experiences. Unreal's Blueprint visual scripting system allows developers to create complex gameplay mechanics without extensive programming knowledge.

However, Unreal Engine has a steeper learning curve compared to Unity, and its focus on high-end graphics and performance makes it more resource-intensive. As a solo developer with limited experience, I determined that Unreal might be more suitable for larger, well-established game development teams working on big-budget project

Godot is a free and open-source game engine that has gained popularity in recent years. It offers a lightweight and efficient development environment, making it an attractive choice for indie developers and small teams. Godot uses its own scripting language called GDScript, which is similar to Python in syntax, making it relatively easy to learn for developers with Python experience.

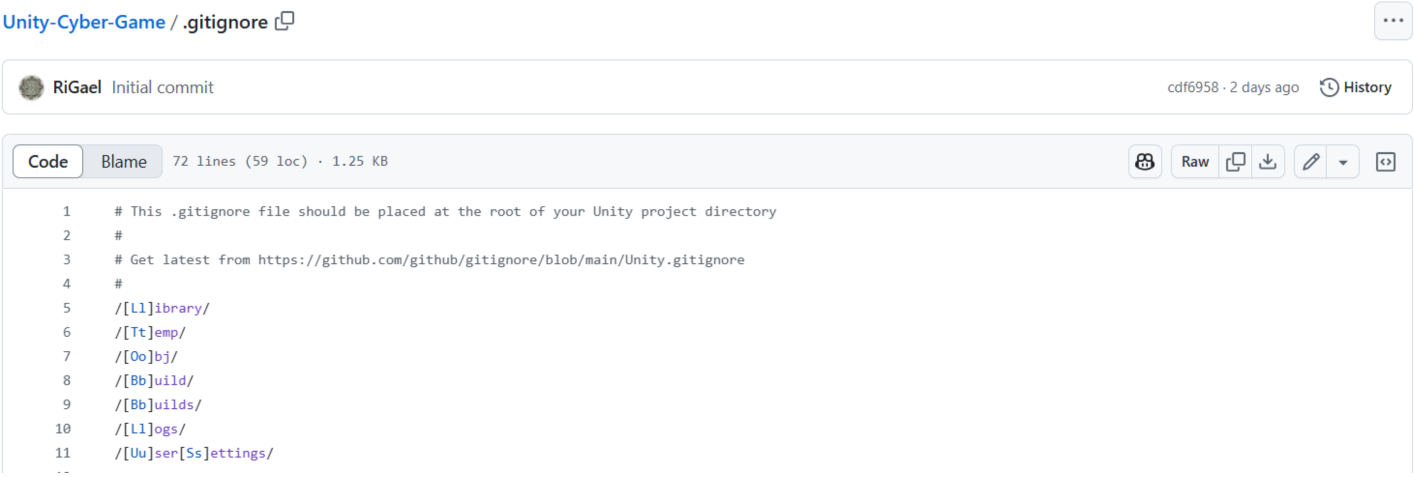
Godot's node-based architecture and intuitive scene system make it easy to create and manage game objects and their relationships. The engine also provides a comprehensive set of tools for 2D and 3D game development, including a built-in editor, animation system, and physics engine.

While Godot is a capable engine, it may have a smaller community and fewer learning resources compared to Unity. Additionally, Godot's focus on efficiency and simplicity may limit its flexibility and extensibility for more complex projects. As can be seen by numerous posts on godotforums about developers complaining bout it’s limitations. (godotforums.org, n.d.)

GitHub

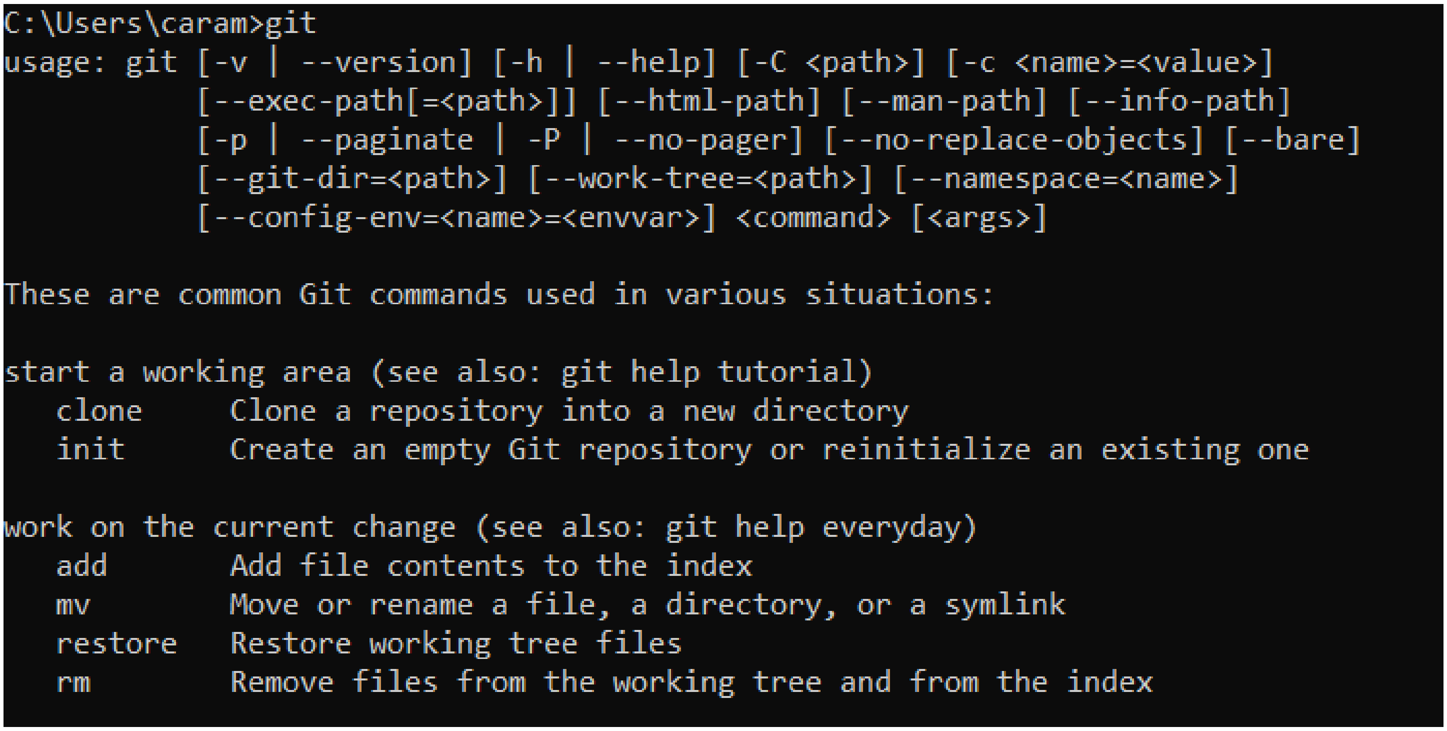
I also intend to use GitHub and to open source my project and all its assets at the end of the development cycle. Thie GitHub link can be found here: https://github.com/RiGael/Unity-Cyber-Game

GitHub provides an integrated gitme file specifically for unity. The Unity .gitignore file is designed to exclude unnecessary files and directories from version control, ensuring that only relevant project files are tracked and pushed to the repository. By utilising this I can get GitHub to ignore build artifacts, temporary files, and system-generated files that are not essential to the project's source code. I can also avoid the repository being littered with large files, such as compiled assets. Ensure that sensitive information, such as API keys or configuration files, is not inadvertently pushed to the public repository.



```
# This .gitignore file should be placed at the root of your Unity project directory
#
# Get latest from https://github.com/github/gitignore/blob/main/Unity.gitignore
#
/[Ll]ibrary/
/[Tt]emp/
/[Oo]bj/
/[Bb]uild/
/[Bb]uilds/
/[Ll]ogs/
/[Uu]ser[Ss]ettings/
```

I will also utilise Github’s in built pull and push commands in order to track changes and the development history of my game.



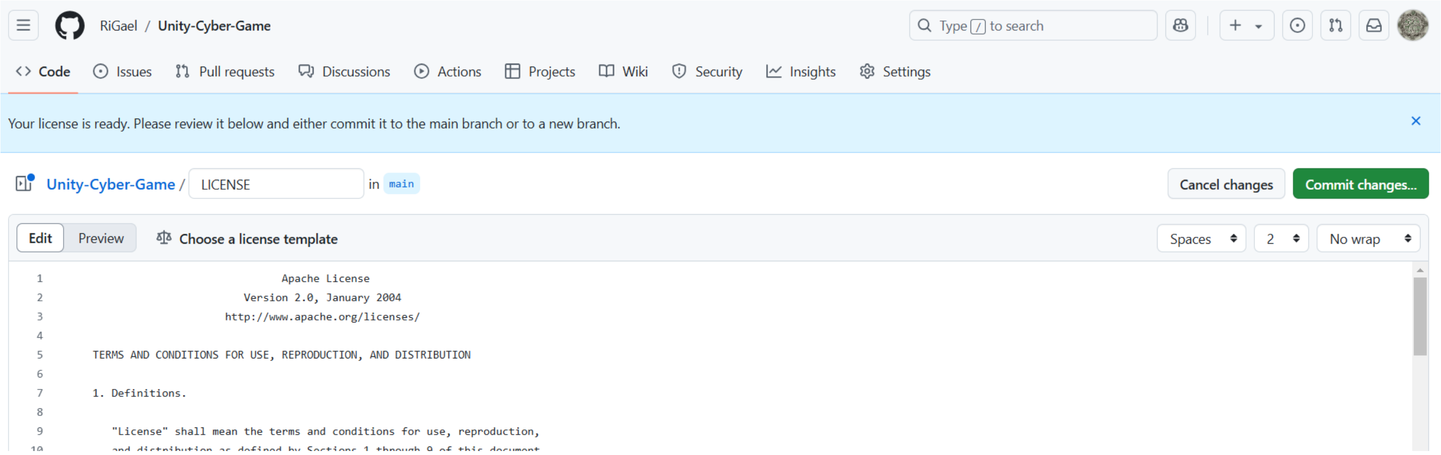
```
C:\Users\caram>git
usage: git [-v | --version] [-h | --help] [-C <path>] [-c <name>=<value>]
           [--exec-path[=<path>]] [--html-path] [--man-path] [--info-path]
           [-p | --paginate | -P | --no-pager] [--no-replace-objects] [--bare]
           [--git-dir=<path>] [--work-tree=<path>] [--namespace=<name>]
           [--config-env=<name>=<envvar>] <command> [<args>]

These are common Git commands used in various situations:

start a working area (see also: git help tutorial)
   clone      Clone a repository into a new directory
   init       Create an empty Git repository or reinitialize an existing one

work on the current change (see also: git help everyday)
   add        Add file contents to the index
   mv         Move or rename a file, a directory, or a symlink
   restore    Restore working tree files
   rm         Remove files from the working tree and from the index
```

Github will also help to educate similar educators and students in the future should they wish to analyse my game code and perhaps learn something from it or utilise my own code for it as I intend to use the The Apache License 2.0, a permissive licence which will allow users to freely use, modify, and distribute your project's code and assets. I have included the LICENCE.md file in my code.



Your license is ready. Please review it below and either commit it to the main branch or to a new branch.

```
                                 Apache License
                           Version 2.0, January 2004
                        http://www.apache.org/licenses/

   TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

   1. Definitions.

      "License" shall mean the terms and conditions for use, reproduction,
      and distribution as defined by Sections 1 through 9 of this document
```

C# Programming language

C# (pronounced as "C Sharp") is a modern, object-oriented programming language developed by Microsoft as part of the .NET framework. It is widely used for developing a variety of applications, including desktop software, web services, and video games. C# is the primary scripting language used in Unity for defining game logic, user interactions, and AI behaviors.

One of the key strengths of C# is its comprehensive set of features that support object-oriented programming (OOP) paradigms. OOP allows developers to organize code into reusable, modular units called classes, which encapsulate data and functionality. C# provides robust support for essential OOP concepts such as encapsulation, inheritance, and polymorphism, enabling developers to write clean, maintainable, and scalable code.

C# also offers a rich set of built-in data types, control structures, and libraries that streamline game development tasks. It has native support for common data structures like arrays, lists, and dictionaries, as well as powerful features such as LINQ (Language Integrated Query) for querying and manipulating data collections. C#'s type safety and exception handling mechanisms help catch errors early in the development process and ensure code reliability.

Another advantage of C# is its active and vibrant developer community. As one of the most popular programming languages worldwide, C# has a vast ecosystem of libraries, frameworks, and tools that extend its capabilities and simplify complex tasks. The Unity Asset Store, for example, offers a wide range of pre-built scripts, plugins, and extensions that can be easily integrated into Unity projects, saving developers significant time and effort.

A 2022 blogpost highlights why C# was chosen for Unity, “The story starts 17 years ago, when our CTO started leveraging the Mono .NET runtime with C#. Unity favored C# due to its simplicity, combined with a JIT (just-in-time) compiler that translates your C# into relatively efficient native code.” (Unity, 2022)

C++ and Godot Comparison

In comparison to C#, C++ is a lower-level, more complex programming language that is often used in Unreal Engine development. C++ provides developers with more direct control over memory management and hardware resources, which can lead to better performance in large-scale, resource-intensive games. However, this level of control also comes with a steeper learning curve and a higher likelihood of introducing bugs and memory-related issues. Unreal Engine's use of C++ caters to developers who prioritize performance and low-level control, but it may be more challenging for beginners or those accustomed to higher-level languages like C#.

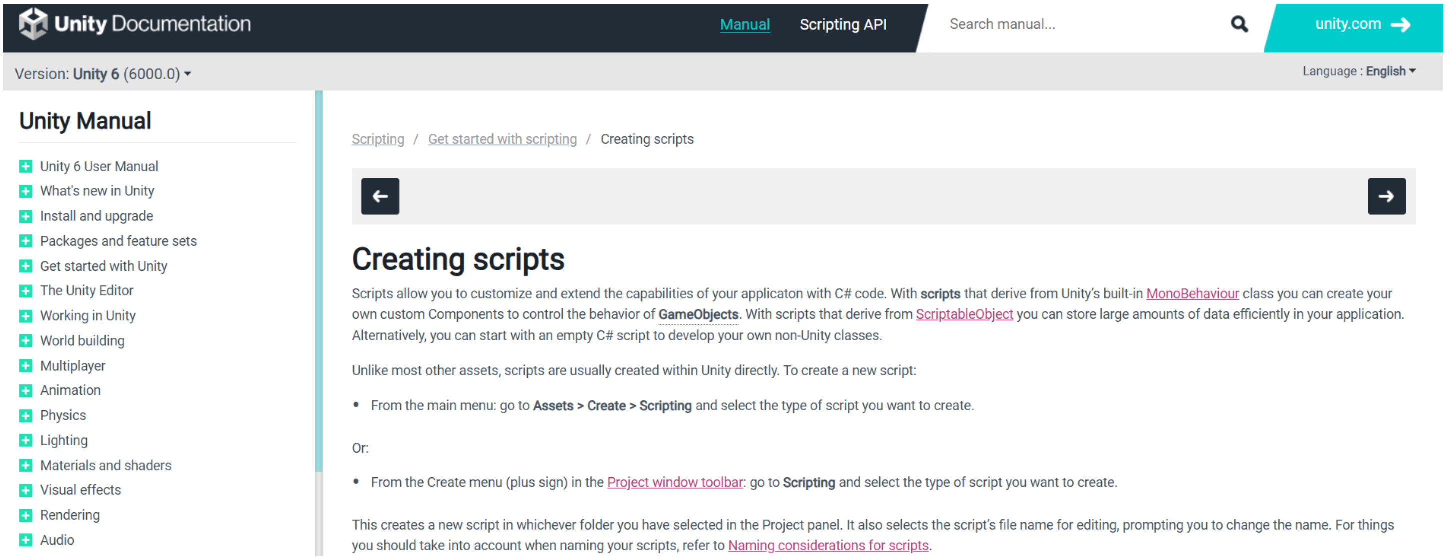
On the other hand, Godot uses its own scripting language called GDScript, which is similar to Python in its syntax and simplicity. GDScript is designed to be beginner-friendly and easy to learn, making it an attractive choice for developers who are new to game development or those who prefer a more streamlined scripting experience. However, GDScript may not have the same level of performance as C# or C++, and it may be less suitable for complex, large-scale projects that require more advanced features and optimizations.

Unity Manual and API

The Unity Manual is a comprehensive online documentation resource that provides in-depth guidance on every aspect of Unity game development. It covers a wide range of topics, from basic concepts like game objects and components to advanced features such as physics simulation, shader programming, and multiplayer networking. (Unity, n.d.)

One of the key sections of the Unity Manual relevant to this research document is the "Scripting" section, which delves into the use of C# for implementing game logic and interactivity. It provides detailed explanations and code samples for essential scripting concepts such as variables, functions, classes, and inheritance.

Here's a screenshot from the Unity Manual's Scripting section, showing how to create scripts in UNITY.



Creating scripts

Scripts allow you to customize and extend the capabilities of your applicaton with C# code. With **scripts** that derive from Unity's built-in MonoBehaviour class you can create your own custom Components to control the behavior of **GameObjects**. With scripts that derive from ScriptableObject you can store large amounts of data efficiently in your application. Alternatively, you can start with an empty C# script to develop your own non-Unity classes.

Unlike most other assets, scripts are usually created within Unity directly. To create a new script:

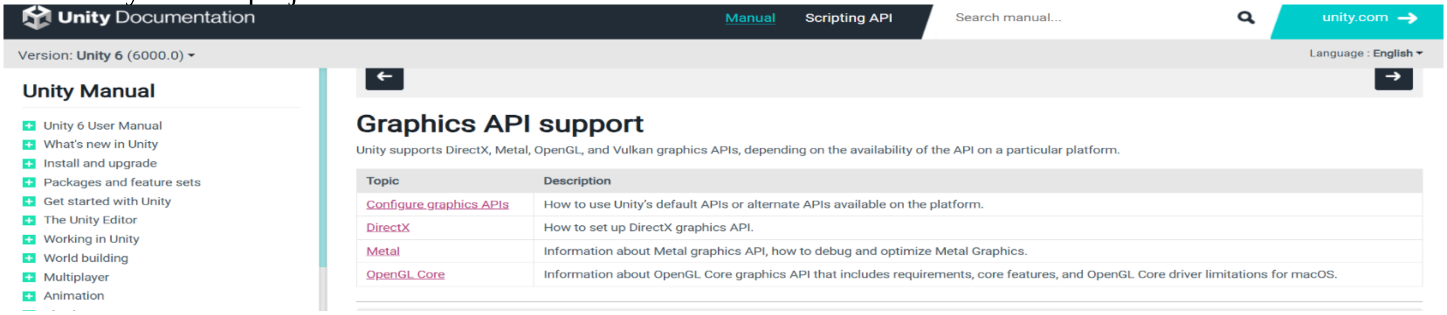
- From the main menu: go to **Assets** > **Create** > **Scripting** and select the type of script you want to create.

Or:

- From the Create menu (plus sign) in the Project window toolbar: go to **Scripting** and select the type of script you want to create.

This creates a new script in whichever folder you have selected in the Project panel. It also selects the script's file name for editing, prompting you to change the name. For things you should take into account when naming your scripts, refer to Naming considerations for scripts.

In addition to the scripting documentation, the Unity Manual also provides extensive information on the Unity API (Application Programming Interface). The API encompasses all the classes, methods, and properties that developers can use to interact with the Unity engine and build game functionality. The manual offers detailed descriptions and usage examples for each API element, helping developers understand how to leverage them effectively in their projects

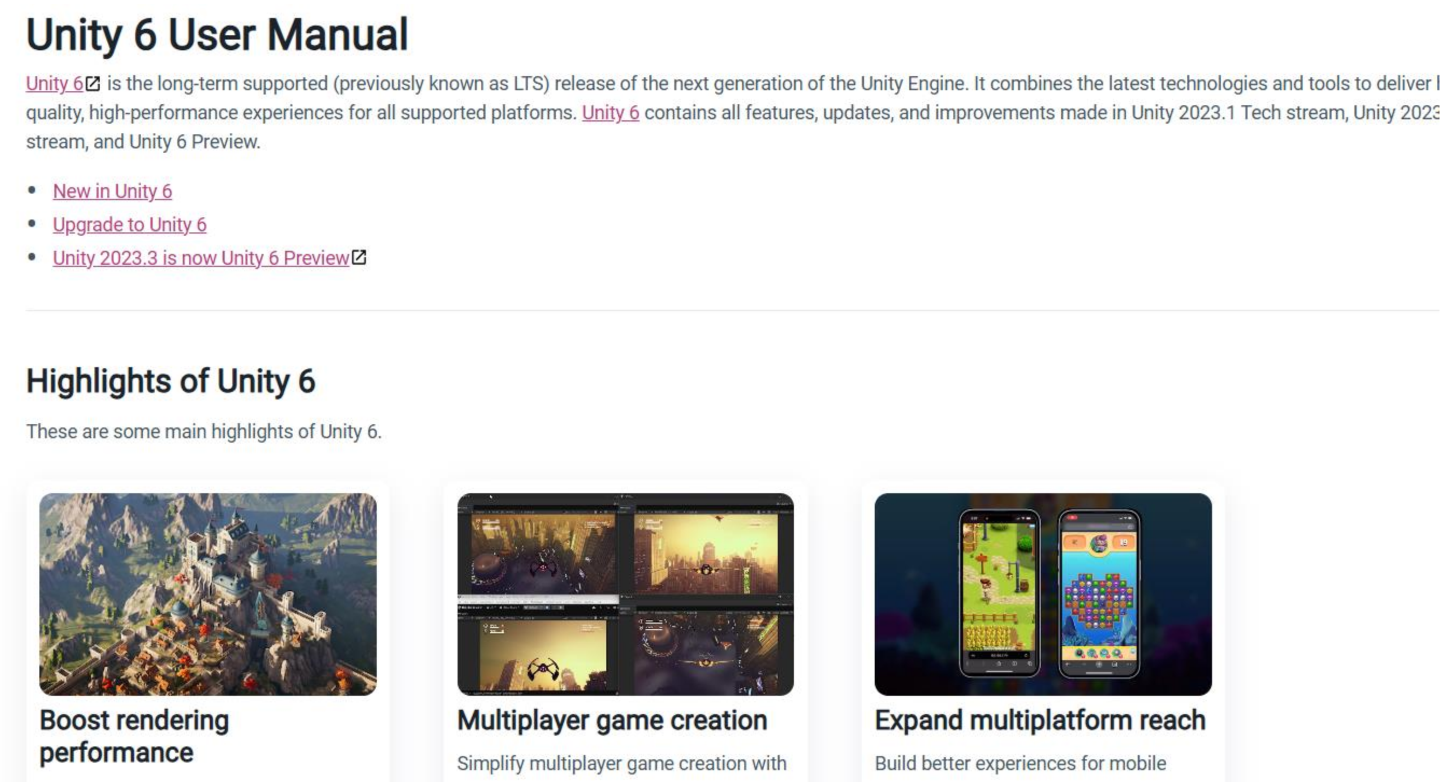


Graphics API support

Unity supports DirectX, Metal, OpenGL, and Vulkan graphics APIs, depending on the availability of the API on a particular platform.

Topic	Description
Configure graphics APIs	How to use Unity's default APIs or alternate APIs available on the platform.
DirectX	How to set up DirectX graphics API.
Metal	Information about Metal graphics API, how to debug and optimize Metal Graphics.
OpenGL Core	Information about OpenGL Core graphics API that includes requirements, core features, and OpenGL Core driver limitations for macOS.

Another valuable resource within the Unity Manual is the "Unity User Manual" section, which provides step-by-step instructions and best practices for working with the Unity Editor interface, asset management, scene setup, and other essential workflows. It includes rich visual aids, GIFs, and videos that demonstrate key concepts and techniques, making it easier for developers to grasp and apply them in their own projects.



Unity 6 User Manual

Unity 6 is the long-term supported (previously known as LTS) release of the next generation of the Unity Engine. It combines the latest technologies and tools to deliver l quality, high-performance experiences for all supported platforms. Unity 6 contains all features, updates, and improvements made in Unity 2023.1 Tech stream, Unity 2023 stream, and Unity 6 Preview.

- New in Unity 6
- Upgrade to Unity 6
- Unity 2023.3 is now Unity 6 Preview

Highlights of Unity 6

These are some main highlights of Unity 6.

Boost rendering performance

Multiplayer game creation

Simplify multiplayer game creation with

Expand multiplatform reach

Build better experiences for mobile

The Unity Manual will prove to be a valuable asset in my journey of building this game from scratch.

Unity Asset Store

The Unity Asset Store is a digital marketplace where developers can find a wide variety of pre-made assets, tools, and plugins to enhance their Unity projects. It serves as a central hub for the Unity developer community to share and acquire high-quality content, saving time and effort in the game development process. By leveraging the Unity Asset Store, I can enhance my cybersecurity training game with high-quality assets, saving development time and effort. The store's extensive collection of pre-made content will allow me to focus on the core gameplay mechanics, educational content, and user experience, while still achieving a polished and visually appealing result.

Assets acquired from the Unity Asset Store can be easily imported and integrated into Unity projects. The Unity Editor provides a streamlined workflow for browsing, purchasing, and downloading assets directly within the development environment. This seamless integration ensures a smooth and efficient asset management process.

Some potential assets that I could consider acquiring from the Unity Asset Store include:

- 3D character models and animations for representing employees, attackers, and other game characters
- Environment assets, such as office spaces, server rooms, and virtual networks, to create immersive and realistic settings
- User interface elements, such as menus, dialog boxes, and information displays, to enhance the game's usability and visual appeal
- Audio assets, including sound effects and background music, to create an engaging and immersive audio experience

- Scripting libraries and plugins that facilitate the implementation of specific game mechanics, such as dialogue systems, inventory management, or puzzle generation

By strategically incorporating assets from the Unity Asset Store, I can accelerate the development process, achieve a higher level of visual and functional quality, and deliver a more engaging and impactful cybersecurity training experience.

Conclusion

In conclusion, the development of a cybersecurity educational training video game has the potential to help and be another weapon in an organization’s arsenal in how they approach employee cybersecurity awareness and training. By leveraging the power of gamification and interactive learning, this project aims to create an engaging and immersive experience that effectively communicates critical cybersecurity concepts and best practices to a diverse audience.

The research conducted highlights the pressing need for improved cybersecurity training, as evidenced by the alarming statistics on data breaches caused by human error and the lack of comprehensive training programs in many organizations across the European Union. The analysis of existing gamified cybersecurity training solutions, such as CYBRScore, Hacknet, CyberEscape Online, and CyberCIEGE, provides valuable insights into the potential of game-based learning in this domain.

The proposed game design and gameplay elements, encompassing a wide range of cybersecurity topics such as social engineering, phishing emails, password security, insider threats, and emerging threats, demonstrate a commitment to creating a comprehensive and practical learning experience. By incorporating engaging storylines, interactive puzzles, and real-world scenarios, the game aims to foster critical thinking, problem-solving, and decision-making skills that are essential for employees to effectively combat cyber threats.

The choice of the Unity game engine as the technological foundation for this project is well-justified, given its user-friendly interface, extensive documentation, and active community support. The utilization of GitHub for version control and open-source collaboration further enhances the project's transparency and potential for future growth and improvement.

However, I also acknowledge the significant challenges that lie ahead, particularly for a solo developer with limited game development experience. These challenges include the steep learning curve associated with mastering the Unity engine and C# programming language, effective time management and project planning, asset development, and striking the right balance between realism and simplicity to cater to a diverse target audience.

Despite these challenges, the potential benefits of this project far outweigh the obstacles. By successfully developing and deploying this cybersecurity educational training video game, organizations can foster a culture of cybersecurity awareness, empower their employees to become the first line of defence against cyber threats, and ultimately strengthen their overall cybersecurity posture.

In summary, by harnessing the power of gamification and interactive learning, this cybersecurity educational training video game has the potential to increase the Cybersecurity posture and boost Cybersecurity awareness of organisations both small and large through the interactive form of a videogame.

References

cisecurity, n.d. *cisecurity.* [Online]
Available at: https://www.cisecurity.org/services/cis-cybermarket/sans-netwars-continuous
[Accessed 01 11 2024].

ENISA, 2024. *https://www.enisa.europa.eu.* [Online]
Available at: https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-executive-summary
[Accessed 03 11 2024].

Eurobarometer, 2024. *https://digital-skills-jobs.europa.eu/.* [Online]
Available at: https://digital-skills-jobs.europa.eu/en/latest/news/eu-faces-growing-cybersecurity-skills-gap-new-eurobarometer-reveals#:~:text=The%20Eurobarometer%20survey%20revealed%20several,awareness%20programs%20for%20their%20employees.
[Accessed 02 11 2024].

europol, n.d. *europol.europa.eu.* [Online]
Available at: https://www.europol.europa.eu/publications-events/publications/malicious-uses-and-abuses-of-artificial-intelligence
[Accessed 11 11 2024].

godotforums.org, n.d. *godotforums.* [Online]
Available at: https://godotforums.org/d/36271-godot-the-good-the-bad-and-the-ugly
[Accessed 10 11 2024].

ibm.com, n.d. *icm.* [Online]
Available at: https://www.ibm.com/topics/insider-threats
[Accessed 11 11 2024].

icasa.org, n.d. [Online]
Available at: https://www.isaca.org/resources/reports/state-of-cybersecurity-2022
[Accessed 11 11 2024].

Knowbe4, n.d. *knowbe4.* [Online]
Available at: https://blog.knowbe4.com/88-percent-of-data-breaches-are-caused-by-human-error
[Accessed 01 11 2024].

Scholefield, S., n.d. *Gamification Techniques for Raising Cyber.* [Online]
Available at: https://arxiv.org/pdf/1903.08454
[Accessed 11 11 2024].

Unity, 2022. *Unity.com.* [Online]
Available at: https://unity.com/blog/engine-platform/unity-and-net-whats-next
[Accessed 30 10 2024].

Unity, n.d. *unity3d.com.* [Online]
Available at: https://docs.unity3d.com/6000.0/Documentation/Manual/UnityManual.html
[Accessed 02 11 2024].