MJoSHT
Malaysian Journal of Science, Health & Technology
[mjosht.usim.edu.my]

Penerbit USIM PRESS

*Article*

# CYBERLEAP: The Planning Process for the Security Awareness Game

Nur Anis Aqilah Binti Muhamad Azahar[1], Nurdiana Azizan[1], Noraizah Abu Bakar[2] and Dini Onasis[3]

[1]*Faculty of Science and Technology, Universiti Sains Islam Malaysia, 71800, Nilai, Negeri Sembilan, Malaysia.*

[2]*Faculty of Accountancy, Universiti Teknologi MARA (UiTM) Cawangan Johor Kampus Segamat Jalan Off KM 12 Jalan Muar, 85000 Segamat, Johor Darul Takzim, Malaysia.*

[3]*Faculty of Economics and Business, Universitas Lancang Kuning (UNILAK), JI. Yos Sudarso, KM. 8, Rumbai, Pekanbaru, Riau, Indonesia.*

*Correspondence should be addressed to:*
*Nurdiana Azizan; nurdiana@usim.edu.my*

*Article Info*
*Article history:*
*Received:10 November 2024*
*Accepted: 20 December 2024*
*Published: 24 February 2025*

*Academic Editor:*
*Azira Khalil*

*Malaysian Journal of Science, Health & Technology*

*MJoSHT2025, Volume 11, Issue No. 1*
*eISSN: 2601-0003*

*https://doi.org/10.33102/mjosht.v11i1.457*



***Abstract*— This paper presents the planning process for CyberLeap, a security awareness game for adolescents. In today's digital age, adolescents navigate a world filled with both opportunities and threats. CyberLeap adopts a novel approach to cybersecurity education in recognition of the significance of providing youngsters with the necessary skills to navigate safely (aligned with Sustainable Development Goals (SDG) 4: Quality Education and 16: Peace, Justice, and Strong Institutions). This casual online game is aimed towards teenagers, drawing them in with interactive tasks that simulate real-life situations, such as password management and phishing attempts. CyberLeap makes learning enjoyable, whether by solving a challenging quiz on secure password creation or identifying a phishing email that appears legitimate. CyberLeap is an educational and entertaining platform that empowers teenagers to become responsible digital citizens by providing a range of tasks, clear feedback explaining correct and incorrect responses, and a rewarding system with points, awards, or even leaderboards. As a result, there may be a safer online atmosphere due to their increased awareness of cyber threats and the encouragement of appropriate online conduct. In the end, CyberLeap advances a more promising cyber world in which teenagers can prosper and confidently explore the immense possibilities of the internet. The implication of the research suggests that integrating engaging, game-based cybersecurity education like CyberLeap into adolescent learning can significantly enhance digital safety and responsibility, contributing to a more secure online environment and supporting SDGs related to quality education and strong institutions. The research concludes that CyberLeap effectively enhances adolescents' cybersecurity awareness and accountable online behaviour through interactive, game-based learning, fostering a safer digital environment and supporting quality education and strong institutions.***

***Keywords*— Cybersecurity; game; security awareness; adolescence**

## I. INTRODUCTION

In the rapidly evolving digital age, cybersecurity has become a critical issue that affects not just people but also communities and whole countries. The development of the internet has revolutionised communication and information sharing, but it has also brought many security threats [1]. One of the articles titled ‘Cybersecurity Awareness Among the Youngs in Malaysia by Gamification’ [2] asserted that a lack of information of Internet knowledge is to blame for the daily rise in incidents of identity fraud, cyberbullying, online harassment, and other crimes. The severity of the issue is shown by the

increase in cyber threats, including widespread data breaches and identity theft. These dangers impact people directly, making everyone a possible target. They are not just directed at governments or businesses. This reality calls for a thorough comprehension of internet safety precautions. The Sustainable Development Goals (SDGs) of the United Nations (SDGs) include a focus on SDG 4: Quality Education and SDG 16: Peace, Justice, and Strong Institutions) in their efforts to build a brighter future for all. Regretfully, virtual environments can occasionally serve as hotbeds of hostility, with cyberbullying being a recurring issue. Cyberbullies create a hostile online environment by harassing, intimidating, and humiliating people via the use of online platforms.

Despite its primary focus on cybersecurity education, CyberLeap can indirectly help address cyberbullying—a barrier to achieving SDGs such as quality education, peace, justice, and strong institutions. Players who learn to spot manipulative techniques and handle online interactions securely become more responsible digital citizens and less vulnerable to cyberbullying. Pushing players to think about the consequences of their conduct online further develops empathy and may even reduce instances of cyberbullying and promote more polite behaviour. Furthermore, by educating players on reporting cyberbullying and getting assistance, the game can empower people to create safer communities. It can also cultivate healthy online interactions by including features that support polite online communities.

Adolescents are a generation of active adventurers who thrive on the internet, a vast digital frontier. Like any explorer, these digital adventurers explore an extensive and intriguing world but require the appropriate safety equipment. Regretfully, their ignorance of cybersecurity makes them susceptible. Imagine that they may have downloaded malicious files, clicked on misleading links, or inadvertently shared private information. By doing these things, they jeopardise their security and privacy online. In 2021, based on a survey that has been conducted on a group of secondary students by [2] show that 80% of them use the internet at least twice a week, 92.47% of them have social media accounts, and 77% of them do not change their passwords very often. From this survey, most adolescents are already exposed to the internet and probably do not have basic knowledge about security since most do not update or change their passwords often.

On the other hand, according to the article titled ‘Cybersecurity Awareness Among the Youngs in Malaysia by Gamification’, [2] also said that according to the statistics, victims who are most likely to be targeted by cybercrime are often between the ages of 13 and 15 [2]. This emphasises how important it is for adolescents to receive early cybersecurity knowledge. Equipping children with the knowledge and skills to recognize and avoid online threats is crucial. However, this digital generation may not be as receptive to traditional teaching approaches.

Teenagers are naturally drawn to games due to their entertaining, engaging, and interactive nature. Playing video games can help you feel accomplished and like you belong, and it can help you escape the stresses of the real world. Traditional approaches to cybersecurity teaching frequently fail to pique adolescents' attention and hold it. When gamification is used in cyber awareness training, it adds fun and interaction to the learning process, making it more engaging and pleasurable for participants [10]. This contrasts traditional cybersecurity methods, considered boring and unengaging [10]. A generation used to dynamic and interactive encounters finds these unappealing methods, including lengthy lectures or rote memorisation drills. People are exposed to online risks due to this disengagement, which causes a worrying awareness gap in cybersecurity. The conference paper titled ‘The Need for Game-Based Learning Methods to Address Cyber Threats’, as cited by [3], highlights the common belief that cybersecurity is dull and uninteresting, which deters participation. As a result, it would be advantageous to boost the involvement of security training programs [3].

On the other hand, Andrews et al. (2023) stated that although game-based approaches to training do not always provide a solution to all problems with cybersecurity training, they can leverage flow when used in a way that makes the material suitably tricky and exciting [3]. Cybersecurity education may become an engaging and dynamic experience by introducing interactive simulations, scenario-based challenges, and possibilities for real-time decision-making. This helps students better comprehend important ideas and build the critical thinking abilities needed to negotiate the challenges of the online environment successfully. Creating an engaging and captivating cybersecurity education can pique people's attention, promote involvement, and ultimately enable them to take an active role in online safety. This project presents a novel solution that uses gamification: a cybersecurity awareness game created to help adolescents become responsible digital citizens who can comfortably navigate the constantly changing digital world. The research questions for this research are as follows: (a) What are the gaps in the existing security awareness web game? (b) How can CyberLeap be protected from threats? (c) How can CyberLeap be ensured that it works well? This research's objectives are: (a) To identify gaps between the existing security awareness web game. (b) To develop CyberLeap, a secure web game system for adolescents. (c) To conduct user acceptance testing to ensure CyberLeap works.

## II. PROBLEM STATEMENT

### *A. Lack of Engagement*

Despite having good intentions, cybersecurity awareness games for teenagers frequently need help with low player engagement, failing to pique their interest and produce learning that applies to real-world situations. In one of the articles titled “Defining Engagement and Characterizing Engaged-Behaviours in Digital Gaming”, written by [6], they define engagement as an ability to experience feelings, ideas, and thoughts prompted by and directed toward the mediated action to fulfil a specific goal [7]. On the other hand, another article named “Measured Game Engagement” stated that engagement is the level of participation or focus a person devotes to an individual or object over time. Adolescents are sociable beings who enjoy socialising and competitiveness. The study identifies attention, relevance, confidence, and satisfaction as essential design characteristics, given the young age of the target audience [11].

Most games released today emphasise the lonely experience rather than utilising the advantages of friendly rivalry and

social learning. Raising awareness of cybersecurity risks requires education, but those who lack the necessary skills or are unwilling may find the training process tedious [8]. Envision a game without achievements that can be shared with friends, without leaderboards or cooperative challenges. The experience may seem lonely because of this isolation, which, therefore, lessens the attraction. Besides, a visually pleasing game and an engaging narrative are necessary for an entertaining game. Envision an uninteresting cybersecurity game with an awkward User Interface (UI), a formulaic plot, and drab visuals. An uninteresting presentation will rapidly lose the attention of teenagers who are constantly exposed to visually appealing stuff.

### *B. Lack of Latest News*

Cybersecurity awareness games aim to educate teenagers, but one major flaw is that they do not address the most recent online problems. Their ability to effectively prepare kids for the constantly changing world of cybercrime is weakened by this separation. Users and consumers are more susceptible to cyberattacks because there has not been much focus on educating them about cybersecurity [4]. Because of this, hackers are concentrating on taking advantage of the human element. They do this by targeting victims through emails, online chat rooms, ransomware assaults, phishing, and identity theft, among other methods [4]. Cyberthreats are now able to thrive on social networking sites. Imagine a game that fails to warn young players about the risks associated with social engineering techniques on these platforms, such as using fake identities for scams or targeted advertising campaigns that aim to influence their purchases. A significant gap in their cybersecurity understanding results from this ignorance.

### *C. Lack of Behavioural Change*

Adolescent cybersecurity awareness programs that follow traditional methods frequently concentrate only on disseminating knowledge about internet dangers. Researchers have begun experimenting with games to encourage modifications in cybersecurity behaviour. These games have much potential, but research on their efficacy frequently reports just player enjoyment rather than quantifiable learning objectives or results in altered behaviour. Additionally, no causal relationship is seen between design decisions and theory [9]. There are drawbacks to this strategy. Adolescents may underestimate the risks, lose essential details, or not be interested enough to remember the material. Games about cybersecurity provide a vital substitute. Beyond delivering information, they can build exciting experiences by integrating interactive features and gaming mechanisms. Adolescents can learn safe online conduct in a secure setting, sharpen their critical thinking abilities to recognise online hazards and cultivate empathy for the possible repercussions of their actions through these experiences. To give teenagers the skills and routines they need to use the internet securely and responsibly, they must strongly emphasise behaviour modification.

### *D. Lack of Progressive Difficulty*

In 2023, [9] cited that players' interest and flow state might be adversely affected by a bad user experience, an absence of gaming features, or complicated mechanics [7]. Many games use a one-size-fits-all strategy. Consider a teenager who has no prior knowledge of cybersecurity theories. They could be placed into a challenging situation involving sophisticated network security breaches or zero-day vulnerabilities. They quickly lose interest in the game due to the excessive technical language and strange conditions they face. Their ability to progress to more complex issues is hindered by the lack of a beginner-friendly introduction, which keeps them from developing a solid grasp of cybersecurity. To create a more casual gaming experience, consider making a game with numerous stages, each getting harder than the previous. Fundamental ideas like keeping passwords secure and spotting phishing attempts could be the primary subjects of the first levels. Players may encounter increasingly complex scenarios with viruses, network flaws, and social engineering techniques.

## III. SCOPE

This security awareness web game will include the standard login and sign-up form to save the player's progress. After logging in, the player will be directed to the main page of the game, where the player will see a few options: start game, new game, cyber news/info, leaderboard, and settings. Players can click the ‘start game’ button to start the game. The game has obstacles where players need to make their way to the end, and there will be questions or activities about security awareness when they are playing the game. It is a casual game which adolescents, even without cybersecurity knowledge, can play this game. The game is being designed with a progressive difficulty structure in mind. This means that as players progress, they will find each level more challenging than the previous one. The player’s progress will be saved, and the player can track their progress. The ‘Cyber news/info’ button will direct the player to the latest information or news about a cyber-related topic. Additionally, the ‘leaderboard’ button will lead the player to the leaderboard, where the player sees their ranks.

This security awareness web game will not include the complex scenario of cybersecurity concepts since this project aims for adolescents and more casual games. Furthermore, this game will not include multiplayer games and will not have the competitive features that make the player need to compete with another player.

## IV. EXISTING SYSTEM

### *A. Google Interland*

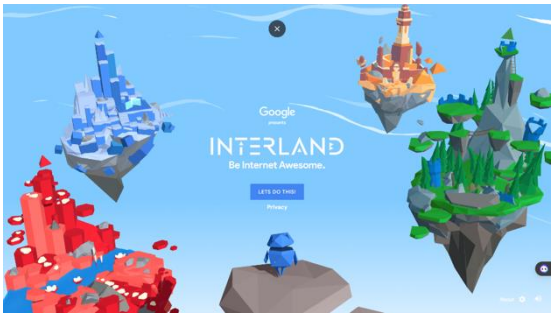

Figure 1. Google Interland Main Page

Google Interland (Figure 1) is a free online treasure from Google's "Be Internet Awesome" campaign that takes youngsters on an exciting internet safety journey. Imagine a fun, three-dimensional environment where kids may explore four exciting activities. Every game offers tasks that impart essential knowledge about digital citizenship. By playing, they will become internet safety experts and have fun simultaneously. There are a few sections that the game has which are:

*1) Reality River:* The terrain (Figures 2 and 3) here could be more precise. Youngsters learn to navigate a flood of pop-ups and hidden information as "Internet Detectives." Youngsters will learn to distinguish between reality and fiction on the internet by recognising phishing schemes and false information.

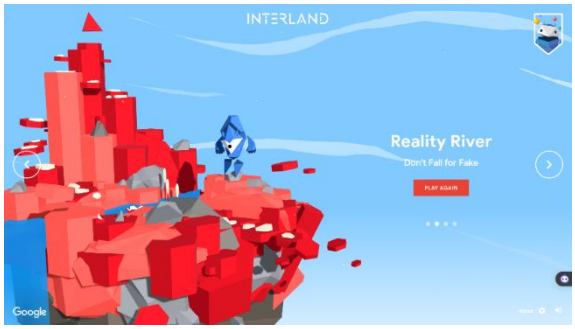

Figure 2. Reality River Page

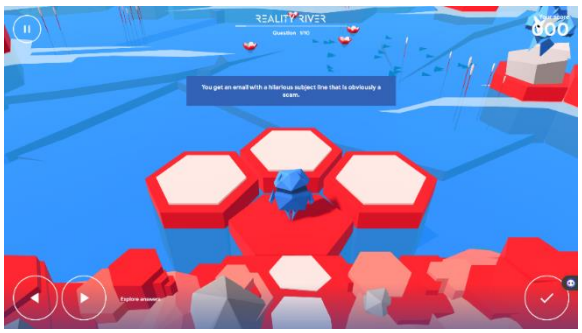

Figure 3. Reality River Game Page 1

*2) Kind Kingdom:* Every kingdom (Figure 4, Figure 5, and 6) is not made equally. Adolescents learn to be representatives of kindness in the Kind Kingdom. Through enjoyable assignments, learners discover the value of online manners, how to confront cyberbullies, and how to disseminate kindness online.

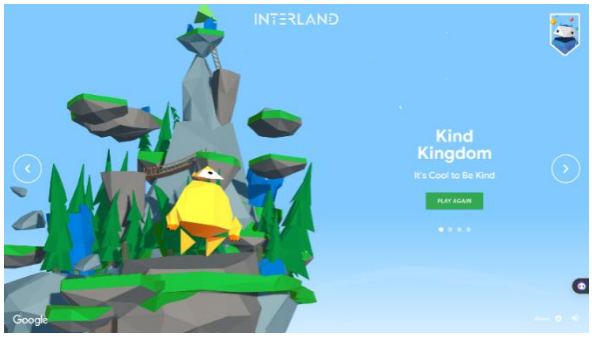

Figure 4. Kind Kingdom Page

Figure 5. Kind Kingdom Game Page 1

Figure 6. Kind Kingdom Game Page 2

*3) Mindful Mountain:* Sorting, not climbing, is the purpose of this mountain. Children volunteer to be "Information Sharers" on Mindful Mountain (Figure 7, Figure 8 and Figure 9) wherever they encounter many kinds of information. They will learn the value of privacy and create good digital behaviours by making thoughtful decisions regarding what they disclose and with which individuals.

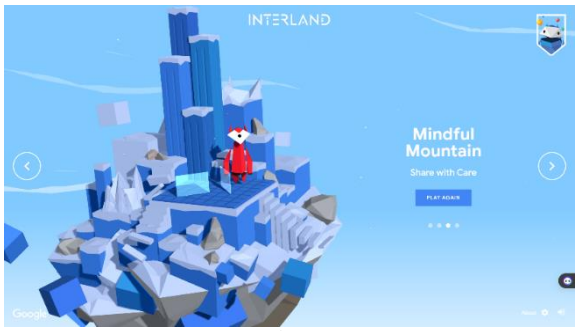

Figure 7. Mindful Mountain Page

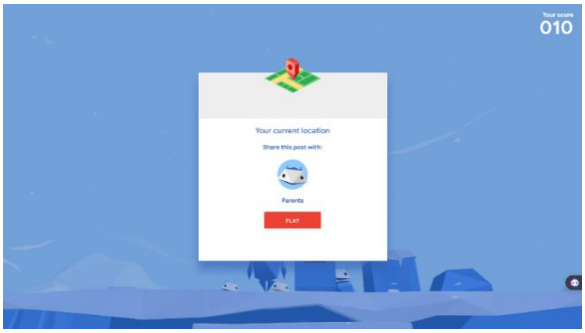

Figure 8. Mindful Mountain Page Game Page 1

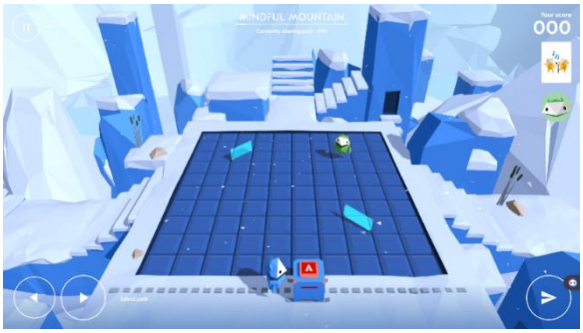

Figure 9. Mindful Mountain Page Game Page 2

*4) Tower of Treasure:* It is crucial to safeguard fortune. adolescents in Tower of Treasure (Figure 10 and Figure 11) become "Password Protectors." They will be faced with riddles and activities that educate kids on the significance of using strong passwords and how to prevent intruders from accessing their internet accounts.

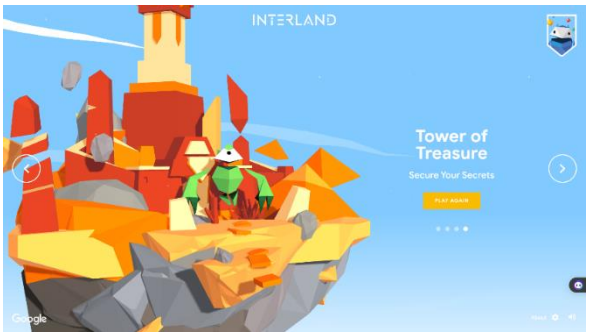

Figure 10. Tower of Treasure Page

Figure 11. Tower of Treasure Game Page

In addition, after all the game sections, the youngster will be provided with quizzes to strengthen their understanding of every topic based on the section.

*B. Cybersecurity Lab*

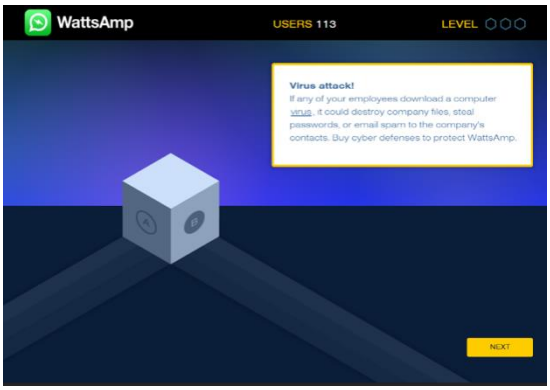

Figure 12. Cybersecurity Lab Main Page

The Cybersecurity Lab (Figure 12 and Figure 13) is a game developed by NOVA in collaboration with cybersecurity professionals. It teaches players about cyber risks and defences and helps them keep their digital lives secure. Players will advance by applying computer code, logic, critical thinking, and vulnerability identification to tackle various issues. Cybersecurity workers frequently use these similar talents. Players in the game operate for a new social network corporation, facing threats from increasingly complex cyberattacks. They aim to expand their small company into a worldwide empire by collaborating with an innovative, astute businesswoman who is also a friend and coworker. Players must accomplish tasks to improve their cyber defences and foil their assailants. The four main gaming elements comprise a password challenge, a social engineering challenge, a coding challenge, and a series of cyber wars.

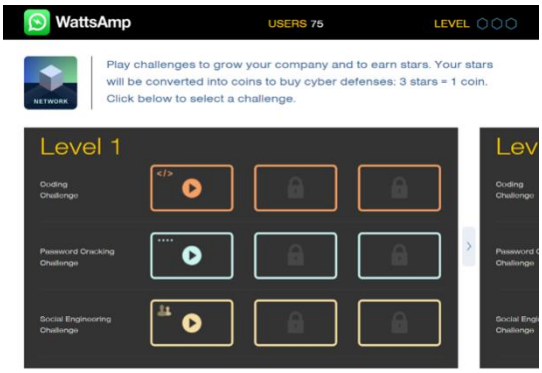

Figure 13. Cybersecurity Lab Level Selection Page

*1) Coding Challenge:* The assignment (Figure 14) introduces computer programming fundamentals. Typically, programming code is written in text. Still, this task uses Blockly, a visual editor made by Google that allows players to construct computer programs by dragging and dropping blocks that stack together. Using Blockly drag-and-drop instructions, players can guide a robot to get through a maze.

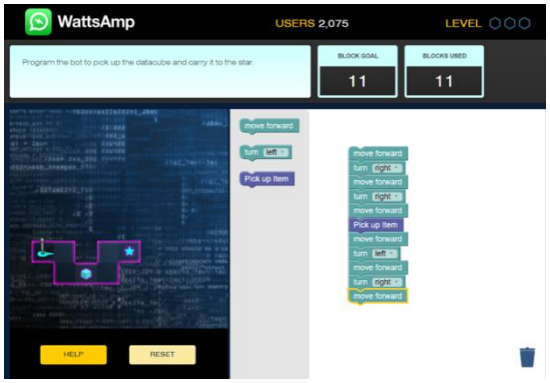


Figure 14. Coding Challenge Page

*2) Password Cracking Challenge:* Since most individuals use passwords (Figure 15 and Figure 16) to verify their identities online, creating and utilising solid passwords is crucial to digital data security. Players must overcome a series of "password duels" to complete the task. These challenges teach participants how password-cracking attacks work and how to develop stronger passwords.

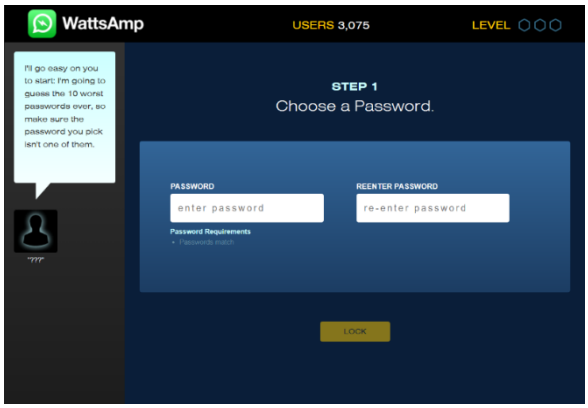


Figure 15. Password Cracking Challenge Page 1

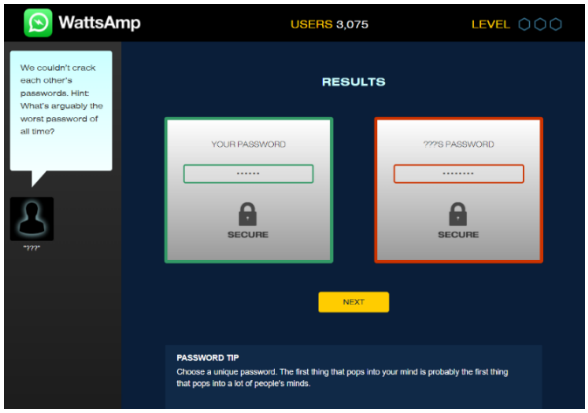


Figure 16. Password Cracking Challenge Page 2

*3) Social Engineering Challenge:* Scammers attempt to fool individuals into sending them emails with malware that contain confidential information (Figure 17). Players will get experience identifying fake emails, websites, and phone calls in this challenge. After completing the task, they will get helpful advice to prevent them from falling for social engineering fraud.

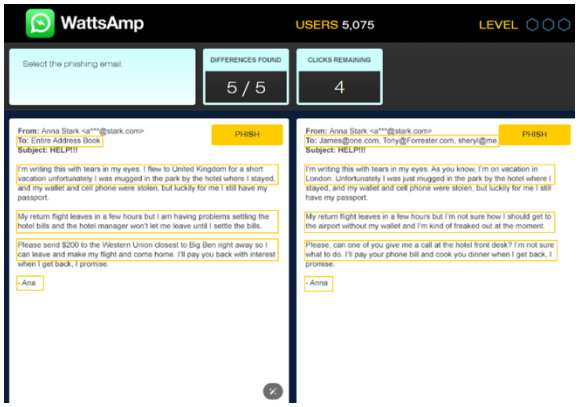


Figure 17. Social Engineering Challenge Page

*4) Network Cyber* Battles By completing the challenges (Figure 18), players will earn resources to buy cyber defences to protect their companies against cyber-attacks that reflect the attacks that actual companies and institutions often fall victim to. Players will learn about cyber-attacks and how to defend institutions from them effectively.

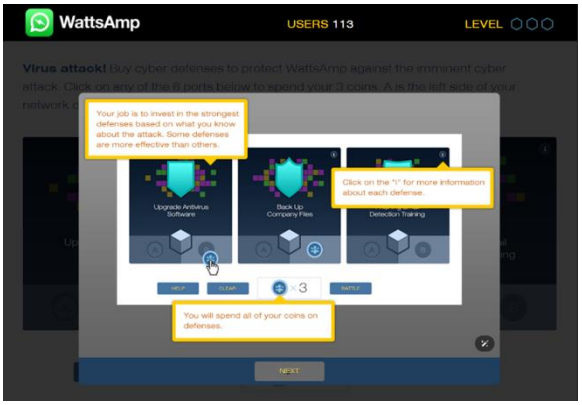


Figure 18. Network Cyber Battles

## *C. CyberCIEGE*


Figure 19. CyberCIEGE Game

CyberCIEGE (Figure 19) is unlike other online games with stages and points. An uninteresting presentation will rapidly lose the attention of teenagers who are constantly exposed to visually appealing stuff. Created by the Naval Postgraduate School, it is a training tool for prospective cybersecurity specialists in organisations such as government agencies,

universities, and specific community colleges. The following summarises how CyberCIEGE aids users in refining their cybersecurity skills:

*1) Scenario Central:* CyberCIEGE's essential component. Pre-built scenarios that mimic actual circumstances experienced by network administrators are shown to users. These situations might include overseeing a small company's network security to protect vital military facilities.

*2) Decision Junctions:* Users encounter crucial decision points in every circumstance. As network administrators, they allocate funds to purchase and configure servers, firewalls, and operating systems, among other hardware and software. Maintaining user productivity while balancing security and financial restrictions is crucial. Users can experience the effects of their judgments in real time as the virtual world adjusts to their decisions.

*3) Attack Simulator:* Security is checked like in the real world. CyberCIEGE unleashes virtualised cyberattacks on you! These assaults might be more complex malware infestations or simple phishing efforts. Users get an understanding of the significance of implementing robust security measures and the repercussions of not doing so by personally witnessing the effects of these assaults.

*4) Feedback Loop:* CyberCIEGE emphasises learning from decisions, not simply making them. Each scenario is followed by comprehensive feedback from the program. This feedback emphasises the significance of any security breaches that may have happened and the effectiveness of the security measures that were put in place. Through this feedback loop, users may improve their ability to make decisions and get a more profound comprehension of cybersecurity best practices.

*D. HotSpot*

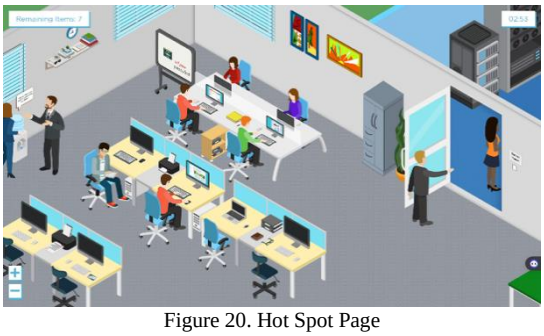

Figure 20. Hot Spot Page

The Hot Spot Cybersecurity Game (Figure 20 and Figure 21) from Living Security is a gamified educational tool that lets users pretend to be cybersecurity experts. Users' task in a virtual workplace is to find and address typical cybersecurity violations. Users may improve their ability to detect and handle cybersecurity hazards in realistic situations by actively identifying and fixing these issues.

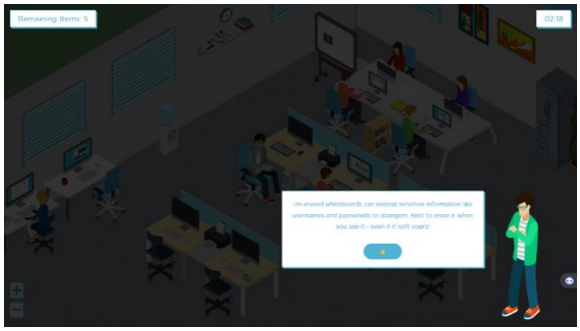

Figure 21. Hot Spot Game Page

## V. COMPARISON TO THE EXISTING SYSTEM

TABLE I. COMPARISON TABLE

| Games | Google Interland | Cyber-security Labs | Cyber-CIEGE | Hot Spot |
|---|---|---|---|---|
| **Type** | WEB | WEB | WEB | WEB |
| **Organisation** | Google | NOVA Lab | NAVAL Post-graduate School | Living Security |
| **Target Audience** | (K-12) 5 – 18 years old | 13+ old | Employee | Employee |
| **Focus** | Anti-Bullying, Internet Safety, Phishing, Information Protection, Cybersecurity Awareness. | Programming (Coding Challenge), Social Engineering, Password Cracking. | Network Security Fundamentals, Risk Management, Security Policies and Procedures, Incidence Response, Physical Security. | Cyber-security Violation. |
| **Rating by Chrome, we store** | 4.4 /5 stars (151 rating) (30 000 users) | 4.4 / 5 stars (21 rating) (881 users) | - | - |
| **Leader Board** | No | No | No | No |
| **Latest News** | No | No | No | No |
| **Overall Graphic** | High | Low | Low | Low |
| **Simulation** | Yes | Yes | Yes | Yes |
| **Casual Game** | Yes | No | No | Yes |

Based on the existing game, most games need better graphics; they rely more on functionality than aesthetics. While this can be understandable, it risks losing players' attention fast, especially adolescents. Engaging visuals can be a powerful tool for keeping players invested, especially when the goal is to ignite their interest in a complex topic like cybersecurity. Throwing some visual flair into the mix could make all the difference in transforming cybersecurity education from a dry chore into an immersive and unforgettable experience. Besides that, they do not implement a leaderboard system in their game. A leaderboard shows the leading competition's names and current scores [9]. Implementing a leaderboard system into the game will increase the player's engagement while playing the game. It is because the leaderboard can create a sense of competition that motivates the players to improve their performance and climb the ranks. In terms of learning about

cybersecurity from the game, players will be encouraged to replay the levels or to complete the challenge to beat their previous score, which will make them learn about their past mistakes and learn to fix them. On the other hand, most of the games below have heavy text content that may make the users, especially adolescents, get bored while playing the game. They need to understand what the game wants, and in some of the games, the user needs to have at least a basic knowledge of cybersecurity to pass the game.

## VI. PASSWORD COMPLEXITY

While security tech keeps evolving, passwords remain the frontline defence. Their strength directly determines how well your data is protected. Despite security technology improvements, passwords remain an essential first line of protection. The degree of difficulty a password is to guess or break using different techniques, such as brute-force assaults or dictionary attacks, is measured by its password complexity [13]. It is frequently connected to specifications for choosing passwords to improve password security [13]. The length of the password can influence the complexity, the character variety used in the password, and the unpredictability. I propose implementing password complexity restrictions to improve the security posture of my security awareness game web-based system.

## VII. METHODOLOGY

Making an excellent web-based game system requires proper and effective planning and methods. SDLC, which stands for Software Development Life Cycle, is an efficient and economical method for designing and creating high-quality software. It provides a roadmap for the entire development process, from the initial concept to deployment and maintenance. With planning, the SDLC aims to reduce project risks and ensure that software fulfils customer expectations during and after production [14].

Many SDLC models exist, such as Waterfall, Agile, Spiral, and Agile Fall. The capacity to change and grow is essential in the dynamic and quick-paced world of game development. This is especially true for web-based game creation, as evolving technology and user expectations make frequent changes. This unstable environment might be challenging for traditional software development approaches, which are frequently inflexible and linear. For the CyberLeap security awareness web-based game, Agile models are chosen to act as a roadmap throughout the developing process.

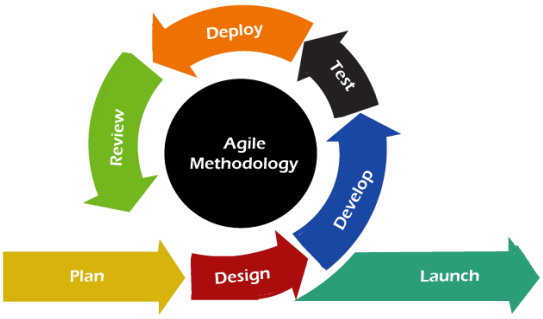


Figure 22. Agile Methodology

Agile development's flexible and iterative methodology welcomes change and fosters ongoing progress. Agile concentrates on producing usable software in brief, iterative sprints, in contrast to traditional approaches with protracted development cycles. This allows testers and users to provide ongoing input, which is subsequently included in new versions. Long development periods and the possibility of producing a subpar product are things of the past when using Agile. To ensure that developers, designers, and other stakeholders are working together towards the same objective of producing a successful web game, Agile is a technique that encourages cooperation.

TABLE II. AGILE PROCESS

| Process | Detail |
|---|---|
| Planning | • Identifying the needs and parameters for the adolescent security awareness game.<br>• Gather information about the target market and industry trends by conducting competitive and market research. |
| Design | • Come up with the idea for the game, the story, and the overall user experience.<br>• Create stages, interactive features, and gaming mechanisms that appeal to the adolescent demographic.<br>• Include learning objectives and security-focused content in the game design.<br>• Create prototypes, mock-ups, and wireframes to illustrate the user interface and gameplay of the game. |
| Develop | • Make sure the development environment and technology stack are established.<br>• Put the user interface, security-related components, and game elements into action.<br>• During development, use safe coding procedures and include security testing.<br>• Apply agile development approaches, which include feedback loops and frequent sprints. |
| Testing | • Perform thorough testing, including user acceptability, integration, and unit tests.<br>• Engage many teenage users in the testing phase to obtain their opinions and ideas.<br>• To find and fix any security flaws, do vulnerability scanning, penetration testing, and security assessments. |
| Deploy | • Optimise the game for the intended platforms and devices to get it ready for release.<br>• Create a thorough deployment strategy considering user onboarding, marketing tactics, and distribution channels.<br>• Provide a scalable infrastructure for the game's analytics, data administration, and hosting. |
| Review | • Track the game's performance, user interaction, and feedback.<br>• Examine user information, trends in behaviour, and game analytics to find areas that need work.<br>• To help shape future improvements, get input from stakeholders such as security experts and teenage users.<br>• Evaluate and reflect after deployment to find best practices and lessons learned. |
| Launch | • Give the teenage players of the game clear instructions and documentation to help them navigate and interact with it.<br>• To resolve users' problems or concerns, provide continuing technical support and customer care. |

## VIII. SYSTEM DESIGN AND ANALYSIS

### *A. Requirement Analysis*

The CyberLeap web game aims to educate and raise awareness about online security while having fun playing the game. The targeted user is an adolescent player from ages 1-18. Ensuring Cyber Gladiators players have a fun and safe experience is critical. We are giving a strict system requirements process top priority to accomplish this. To achieve the project's objectives, it is necessary to thoroughly define the technical specifications required to run the game properly and to guarantee a flawless user experience during acceptance testing. To ensure a smooth development process and a well-received game by players, we have thoroughly examined industry resources, including publications, journals, and news sources. Adhering to these guidelines can provide a secure and exciting online environment for future cybersecurity warriors.

### *B. System Design*

A software system can be constructed according to a thorough blueprint in the system design document. It dissects the system into its fundamental parts, including the database, server-side logic (backend), and user interface (frontend). The way these different parts come together to accomplish the intended capabilities is explained in this text. The objective of the system, the intended audience, and the features that users will interact with are also described in the paper. It also explores the technical details, such as the databases, frameworks, and programming languages utilised in development. The data flow is diagrammed to show how the system changes and user interactions spark activities.

The CyberLeap game is a web-based platform created to provide adolescents (ages 13 to 18) an entertaining and interactive introduction to cybersecurity concepts. Below is a summary of the main elements that will make up the architecture of the system:

- User Interface
- Backend
- Unreal Engine Game Client
- Database

TABLE III. SYSTEM'S USER AND ROLE

| User | Role Description |
|---|---|
| Players | • Sign-up and Login<br>• Profile Management<br>• View Progres Tracking<br>• Following the game story progression<br>• Earning reward |
| Administrators | • Create, Edit and Delete Scenarios<br>• Manage Question and Answer poll.<br>• Update storyline.<br>• View and manage player accounts.<br>• Monitor player Progress.<br>• Address any player concerns or issues |

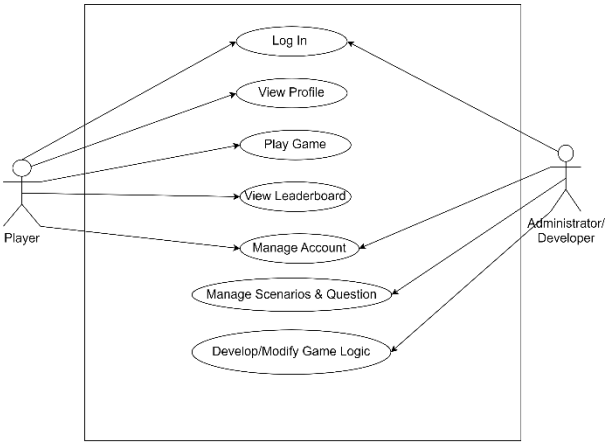


Figure 23. Use Case Diagram

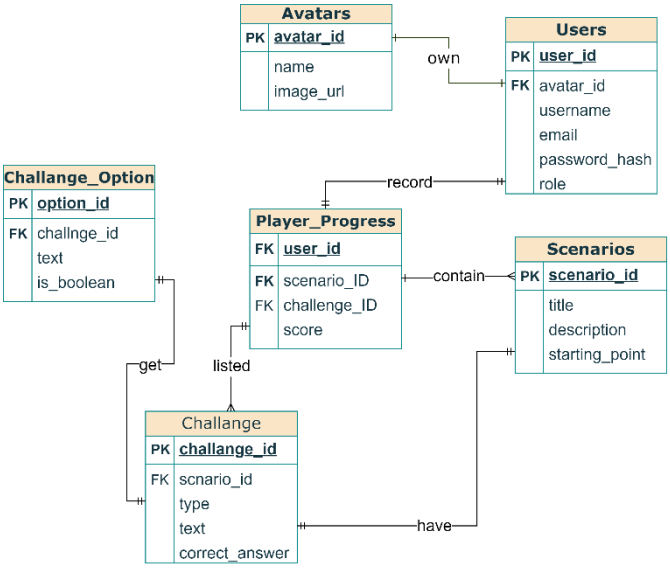


Figure 24. System Data Design

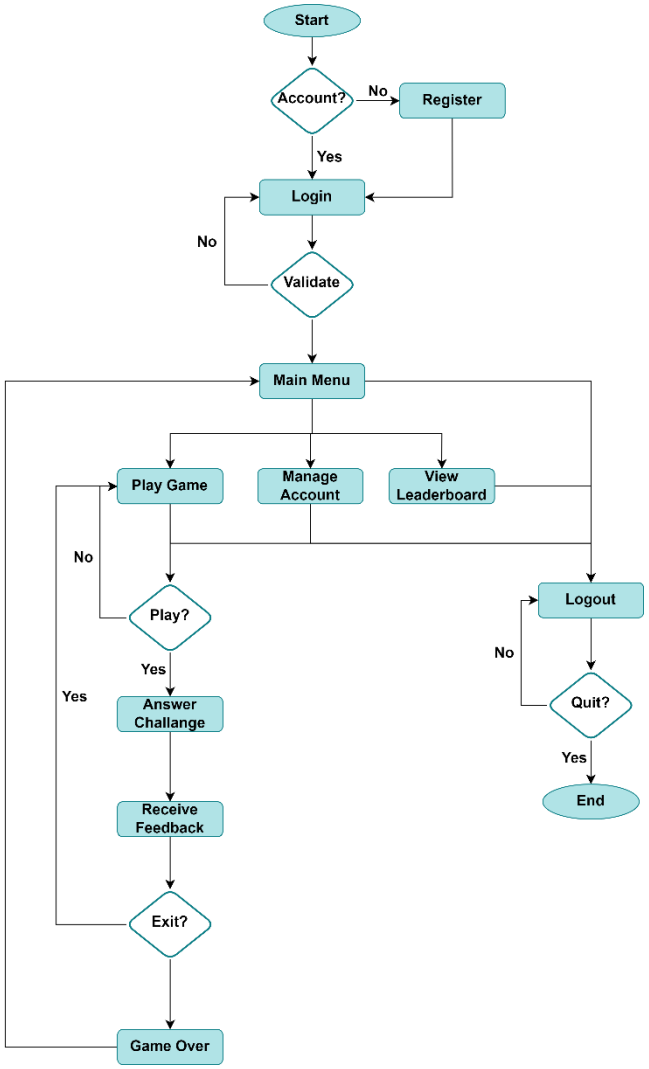


Figure 25. Player's Flowchart

The user will access the main menu after logging in to the game. Users will have a few options on the main menu.

*1) Play Game:* As the player advances through the game's story, they face obstacles and must make decisions.

*2) Answer Challenge:* The player engages with various challenge formats, including minigames, puzzles, and quizzes, and provides solutions.

*3) Receive Feedback:* Along with explanations for right or wrong responses, the player receives feedback on how they performed in the challenges.

*4) View Leaderboard:* The player looks at a leaderboard to assess their progress against other players.

*5) Manage Account:* The player updates basic profile information or resets passwords.

*6) Manage Account:* The player updates basic profile information or resets passwords.

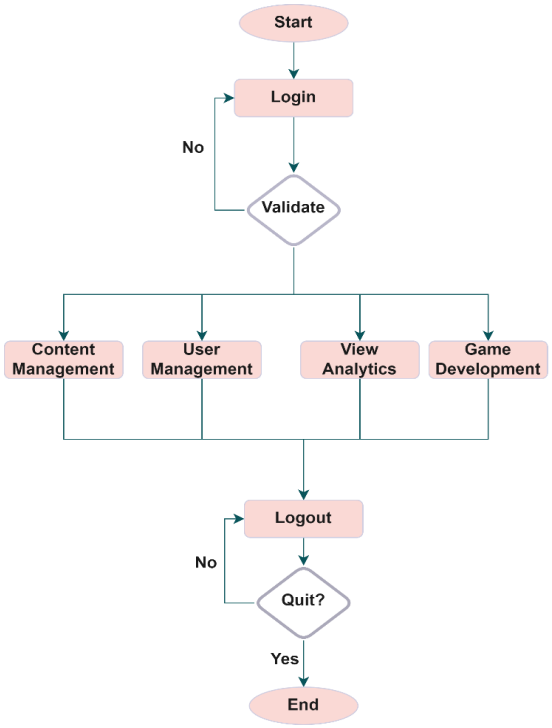


Figure 26. Admin/Developers Flowchart

*1) Content Management:* Created, edited, and deleted situations, including narrative branches and challenges, which are done by the developer/administrator. They can also define response options and feedback processes for creating, editing, and deleting questions about cybersecurity-related subjects.

*2) User Management:* Viewing and managing player accounts, including adding and removing users, changing passwords, and attending to user issues, is the responsibility of the developer/administrator.

*3) View Analytics:* Using analytical tools, the developer/administrator can monitor player performance information and user engagement trends.

*4) Develop Game Logic:* Within the Unreal Engine environment, the developer/administrator may have a use case for changing essential game logic or features.

*5) Logout:* Admin/Developers can log out of the environment after saving the changes.

TABLE IV. WEB GAME-BASED SYSTEM

| **Language/ Tools** | **Description** |
|---|---|
| C++ | Provides the core game development environment with tools for building visuals, gameplay logic, and user interfaces. |
| Unreal Engine | Game Engine |
| MySQL | Database management system |

A thorough testing procedure is necessary to guarantee CyberLeap offers a refined experience. This entails unit testing individual code components, functional testing key gameplay features, performance testing under load, security testing for vulnerabilities, usability testing for user-friendliness, and compatibility testing for compatibility across various devices. With a bug-tracking system and methodical testing throughout development, the team can find and address problems, improve

the game's design, and produce a final product that meets the standards.

Cyber Gladiators require constant upkeep to be sharp, like polishing a gem. This includes resolving problems, introducing new tasks and content, adjusting the difficulty level to ensure fair gameplay, correcting security flaws, maintaining servers, and maximising performance. A web game must have version control, comprehensive documentation, monitoring tools, and active player involvement to be successful over time and give players a consistently good experience.

## IX. RESULT

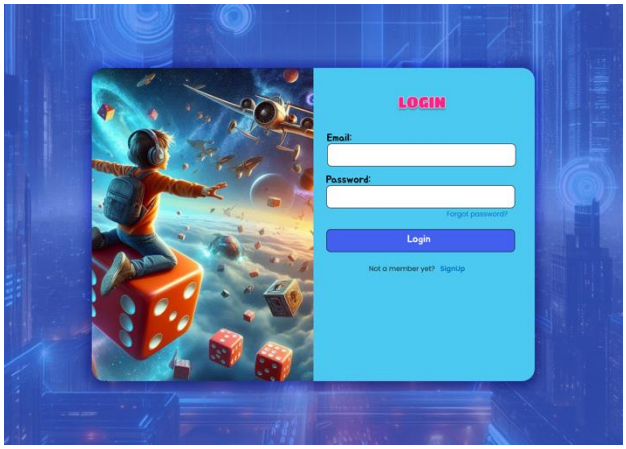


Figure 27. Login Page

Users must enter their login and password on this page in the correct combination, as shown in Figure 27. If the credentials do not match the database that is currently in place, the system will not permit the users to log in. Users will also be able to access the website using a forgotten password option, which allows them to reset their password in case they forget it.

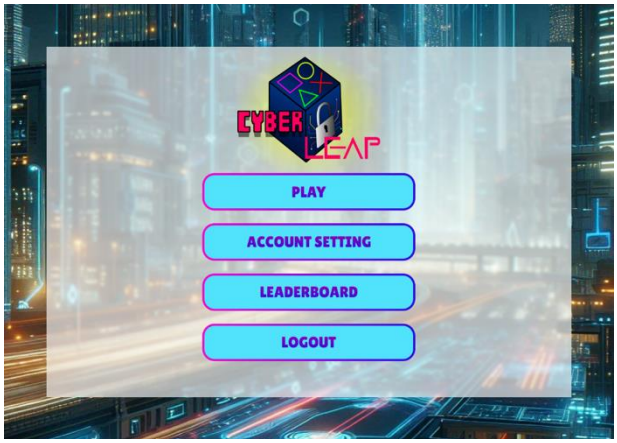


Figure 28. Main Page

On this page, players will have a few operations they can choose from, such as the first play game, where they will directly go to play it. Next is Account Setting, where the User can manage their account. For example, they change passwords, access information, and adjust the game settings. Other than that, it also has the Leaderboard and logout options.

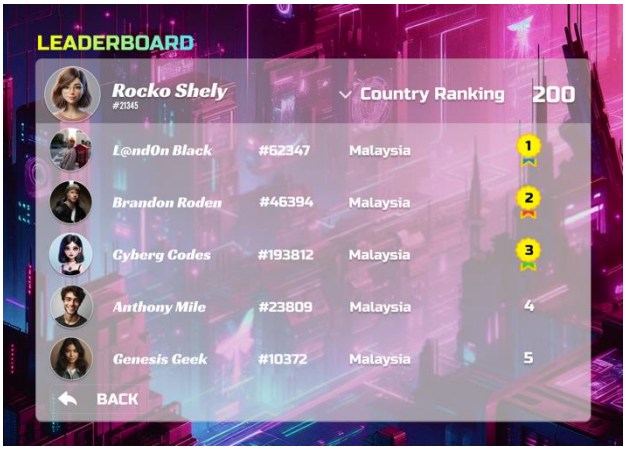


Figure 29. Leaderboard Page

On this leaderboard page, players watch their ranking and the top-ranking score or completion times.

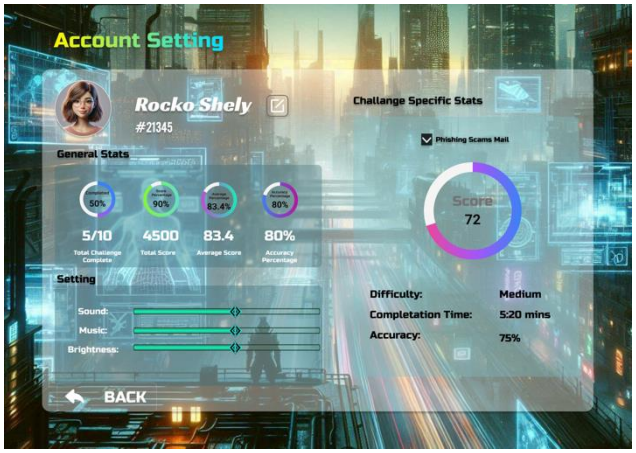


Figure 30. Account Setting Page

On this player, the player can manage their account whether they want to edit their information, change their password, or change/adjust the game settings. They can also view their performance in the game.

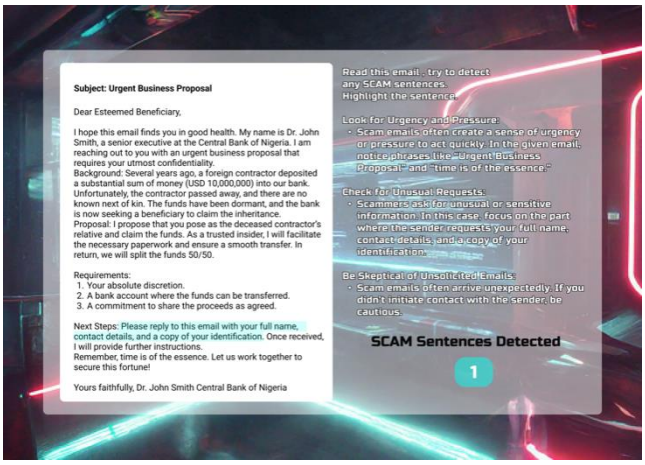


Figure 31. Game Page

This is one of the game challenges that will be held in the game, where the player will answer the question or try to identify what the instructions want. They will receive feedback on whether their answer is correct or not.

## X. CONCLUSION

This paper has provided an overview of a game web-based system and compared a similar existing game web-based system for this project. The comparison is arranged into the table to make it more readable and transparent. The weaknesses and the overview of the existing system are also discussed in this chapter. This paper also discusses the security element which will be implemented in the CyberLeap game. It also discussed the critical gaps that will be used to implement the CyberLeap web-based game system for adolescents.

## CONFLICT OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this paper.


## ACKNOWLEDGEMENT

We thank everyone who provided insight and expertise that greatly assisted the research, although they may disagree with the interpretations and conclusions of this paper. We thank the reviewers, proofreaders, and the handling editor for the comments and assistance that significantly improved the manuscript.


## REFERENCES


[1] Palma, J. C. (2023, May 19). The Internet Revolution: Connecting the World and Changing Lives - Smartencyclopedia. Retrieved May 16, 2024, from Smartencyclopedia - One World of Information website: https://smartencyclopedia.org/2023/05/19/the-internet-revolutionconnecting-the-world-and-changing-lives

[2] Jian, Ng Jia, and Intan Farahana Binti Kamsin. "Cybersecurity Awareness Among the Youngs in Malaysia by Gamification." In 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021), pp. 487-494. Atlantis Press, 2021. doi: 10.2991/ahis.k.210913.061

[3] Andrews, George, Chitra Balakrishna, and Alexander Mikroyannidis. "The Need for Game-Based Learning Methods to Address Cyber Threats." In Proceedings of the 17th European Conference on Game-Based Learning: ECGBL 2023. Academic Conferences and publishing limited, 2023.

[4] Bouvier, Patrice, Elise Lavoué, and Karim Sehaba. "Defining engagement and characterizing engaged-behaviors in digital gaming." Simulation & Gaming 45, no. 4-5 (2014): 491-507. doi: 10.1177/1046878114553571

[5] Batzos, Zisis, Theocharis Saoulidis, Dimitrios Margounakis, Eleftherios Fountoukidis, Elisavet Grigoriou, Achilleas Moukoulis, Antonios Sarigiannidis et al. "Gamification and Serious Games for Cybersecurity Awareness and First Responders Training: An overview." Authorea Preprints (2023). doi: 10.36227//techrxiv.22650952.v1

[6] Bilolova, Zamira Bakhtiyarovna. "Use Of Foreign Experience In Providing Informational Psychological Security Among Youth." Pedagogical Cluster-Journal of Pedagogical Developments 2, no. 1 (2024): 401-409. Retrieved from https://euroasianjournals.org/index.php/pc/article/view/159

[7] Calvano, Miriana, Federica Caruso, Antonio Curci, Antonio Piccinno, and Veronica Rossano. "A Rapid Review on Serious Games for Cybersecurity Education: Are" Serious" and Gaming Aspects Well Balanced?." In IS-EUD Workshops. 2023. https://ceur-ws.org/Vol-3408/short-s3-05.pdf

[8] Chen, Tianying, Jessica Hammer, and Laura Dabbish. "Self-efficacy-based game design to encourage security behavior online." In Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems, pp. 1-6. 2019. doi:10.1145/3290607.3312935

[9] Cambridge Dictionary. (2024). leaderboard. Retrieved May 15, 2024, from @CambridgeWords website: https://dictionary.cambridge.org/dictionary/english/leaderboard

[10] Gwenhure, Anderson Kevin, and Flourensia Sapty Rahayu. "Gamification of cybersecurity awareness for non-it professionals: A systematic literature review." International Journal of Serious Games 11, no. 1 (2024): 83-99. doi: 10.17083/ijsg.v11i1.719

[11] Maathuis, Clara, Frederick Janssens, and Ebrahim Rahimi. "Design of a Disinformation Awareness Digital Game." In A Conference Hosted By. 2024. doi: 10.34190/ecsm.11.1.2053

[12] MDN. (2024, May 6). Website security - Learn web development | MDN. Retrieved May 16, 2024, from MDN Web Docs website: Website security - Learn web development | MDN (mozilla.org)

[13] 1Kosmos. (2023, November 15). Password Complexity: Strengths, Weaknesses, Best Practices. Retrieved May 16, 2024, from 1Kosmos website: https://www.1kosmos.com/security-glossary/password-complexity/

[14] AWS. (2024). What is SDLC? - Software Development Lifecycle Explained - AWS. Retrieved May 16, 2024, from Amazon Web Services, Inc. website: https://aws.amazon.com/what-is/sdlc/#:~:text=The%20software%20development%20lifecycle%20(SDLC,expectations%20during%20production%20and%20beyond