

**Cybersecurity Awareness Game**

**By:**

1. **Mohamad Mohamad 202102248**
2. **Mohamad hussein moussawi 202102313**
3. **Nader othman 202302722**
4. **Hadi Mostafa 202303776**

**Project**

Submitted in Partial Fulfillment of the Requirements for the Degree of Bachelor in………………………….

Department of Electrical and Computer Engineering

Faculty of Engineering

Contents

[List of Figures 6](#_Toc98435774)

[List of Tables 7](#_Toc98435775)

[Project Description 8](#_Toc98435776)

[Project Overview 8](#_Toc98435777)

[Objectives 8](#_Toc98435778)

[Background 8](#_Toc98435779)

[Literature Review 8](#_Toc98435780)

[Applications 8](#_Toc98435781)

[Alternative Designs 8](#_Toc98435782)

[Project Planning 9](#_Toc98435783)

[Constraints 9](#_Toc98435784)

[Project Issues 9](#_Toc98435785)

[Team Members Tasks 9](#_Toc98435786)

[Ethical Issues 9](#_Toc98435787)

[Software Model Process 9](#_Toc98435788)

[Feasibility Study 9](#_Toc98435789)

[Tools/Technology 9](#_Toc98435790)

[Standards 9](#_Toc98435791)

[Milestones 9](#_Toc98435792)

[Requirements 10](#_Toc98435793)

[Use Cases 10](#_Toc98435794)

[Functional Requirements 10](#_Toc98435795)

[Data Requirements 10](#_Toc98435796)

[Non-Functional Requirements 10](#_Toc98435797)

[Design 11](#_Toc98435798)

[Class Diagrams 11](#_Toc98435799)

[Dynamic Model 11](#_Toc98435800)

[Subsystem Decomposition 11](#_Toc98435801)

[Hardware / software mapping 11](#_Toc98435802)

[User Interface 11](#_Toc98435803)

[Test Plans 12](#_Toc98435804)

[Implementation 13](#_Toc98435805)

[Results Evaluation 14](#_Toc98435806)

[Conclusion 15](#_Toc98435807)

[Summary 15](#_Toc98435808)

[Novelty 15](#_Toc98435809)

[Integrity and Values 15](#_Toc98435810)

[Future Work 15](#_Toc98435811)

[References / Bibliography 16](#_Toc98435812)

[Appendix 18](#_Toc98435813)

# List of Figures

Figure 1 - Sample Image of a Survey Dive Boat 11

# List of Tables

Table 1- Sample Table of Survey Dive Activity 11

# Project Description

## Project Overview

In today’s digital age, cybersecurity awareness is essential to protect individuals and organizations from growing cyber threats. This project proposes an interactive game designed to raise awareness about various types of cyberattacks—such as phishing, ransomware, and social engineering—while teaching best practices for prevention. The game simulates realistic attack scenarios and incorporates AI-generated questions and challenges via an API to test and enhance users’ cybersecurity knowledge. This engaging, educational approach is intended to improve individual skills and serve as an effective training tool for organizations and educational institutions.

## Objectives:

## Raise Awareness: Increase understanding of cybersecurity threats and the importance of robust preventive measures.

## Engaging Learning Experience: Provide an interactive, gamified simulation of real-world cyberattack scenarios.

## Continuous Improvement: Utilize dynamic, AI-generated questions that adapt to the user’s performance to reinforce learning.

## Versatility: Offer a tool that can be used for personal self-improvement, corporate training, and integration into educational curricula.

## Background:

## Extensive research into existing cybersecurity awareness tools, educational platforms, and gamification methods informed this project. Discussions with cybersecurity experts and IT professionals helped shape the design and content, ensuring that the game reflects realistic threat scenarios and effective countermeasures. This project addresses gaps found in current tools by combining gamification with dynamic, AI-driven content for a unique, adaptive learning experience.

## Literature Review:

## Top Level View

## Cybersecurity awareness has become a critical issue in the digital age. Traditional methods like seminars and static online courses are giving way to more interactive, engaging approaches. The core challenge lies in effectively engaging diverse audiences—individuals, corporate employees, and students—while presenting complex cyber threat information in an accessible format. Key factors include:

## User engagement and motivation

## Realistic simulation of cyberattack scenarios

## Adaptive learning through AI-generated challenges

## Balancing educational content with gamified interactivity

## Historical Review:

## Early cybersecurity training relied heavily on manual instruction, static presentations, and one-size-fits-all content. Over time, training evolved to include computer-based simulations and online modules. Recently, gamification and interactive learning have emerged as powerful methods to improve retention and practical skills. Research has shown that engaging, game-based learning environments can enhance understanding of complex subjects such as cybersecurity by providing hands-on, simulated experiences.

## Current Trends:

## Recent advancements focus on:

## AI and Machine Learning: Adaptive learning systems now use AI to generate dynamic questions and scenarios, personalizing the training experience.

## Gamification: Points, badges, and leaderboards are increasingly used to motivate learners and sustain engagement.

## Real-Time Simulations: Cyberattack simulations are becoming more realistic, providing users with immediate feedback on their responses.

## User-Centric Design: Modern platforms prioritize intuitive interfaces and customizable learning paths to cater to varying skill levels.

## Relevance to Our Project:

## Our project aims to develop an interactive game that raises cybersecurity awareness by combining realistic cyberattack simulations with AI-generated, adaptive questions. This approach directly addresses the shortcomings of traditional training methods by:

## Engaging users through interactive, gamified scenarios.

## Providing personalized learning experiences that adjust to the user's performance.

## Keeping content current and reflective of the ever-evolving cyber threat landscape.

## \

## Key Themes of Literature:

## Gamification in Cybersecurity Training

## Overview: Gamification leverages game-design elements—such as points, levels, and challenges—to increase motivation and engagement in learning environments.

## Relevance: These techniques are critical for our project, as they transform cybersecurity training from a passive to an active learning experience.

## Studies to Reference:

## “Gamification in Cybersecurity Training: Enhancing Engagement and Learning”

## “Interactive Learning: The Role of Gamification in Modern Education”

## AI-Driven Adaptive Learning

## Overview: AI systems can dynamically generate content and adjust the difficulty of challenges based on user performance.

## Relevance: AI-generated questions ensure that users receive personalized feedback and challenges that are neither too simple nor overwhelming.

## Studies to Reference:

## “Adaptive Learning Systems in Cybersecurity Education”

## “The Impact of Artificial Intelligence on Educational Content Delivery”

## Simulation of Cyberattack Scenarios

## Overview: Realistic simulations are used to mimic actual cyber threats, providing learners with practical, hands-on experience.

## Relevance: By experiencing simulated phishing, ransomware, and social engineering attacks, users can better understand threat indicators and prevention strategies.

## Studies to Reference:

## “Simulation Techniques for Cybersecurity Training”

## “Real-World Cyberattack Simulations as an Educational Tool”

## Challenges in Cybersecurity Training

## Common Challenges: Ensuring up-to-date content, maintaining user engagement, and integrating advanced AI features without overwhelming the learner.

## Relevance: Our project tackles these challenges by focusing on continuous adaptation and user-centered design.

## Studies to Reference:

## “Overcoming Challenges in Cybersecurity Education”

## “Innovative Approaches to Enhance Cybersecurity Awareness”

## Research Gaps and Opportunities:

## Real-Time Adaptation: While many systems offer static content updates, there is a significant opportunity to develop AI-driven modules that adapt in real time to emerging cyber threats.

## Integration of User Preferences: Although personalization is gaining traction, incorporating continuous, real-time user feedback into cybersecurity training remains underexplored.

## Sustained Engagement: Many educational tools struggle with maintaining long-term engagement. Research into more effective gamification strategies could lead to higher completion rates and better learning outcomes.

## Hybrid Approaches: Combining simulation-based learning with AI-driven adaptive content and gamification represents a promising area for further research and innovation.

## Conclusion

## Cybersecurity training has evolved significantly—from traditional classroom lectures to dynamic, interactive simulations. Advanced techniques such as gamification, AI-driven adaptive learning, and real-time simulations are transforming how users learn about cyber threats. However, challenges such as maintaining up-to-date content, integrating real-time user feedback, and ensuring sustained engagement still persist. These challenges also present opportunities for future research and development, particularly in creating hybrid models that combine multiple advanced techniques to deliver a more flexible, scalable, and effective cybersecurity training solution.

## Applications:

## Personal Use: Individuals can use the game to improve their ability to identify and counteract cyber threats.

## Corporate Training: Organizations can integrate the game into employee training programs to bolster cybersecurity defenses and compliance.

## Educational Institutions: Schools and universities can incorporate the game into curricula or workshops to teach cybersecurity fundamentals.

## Alternative Designs:

## The project will be developed as a web application, ensuring accessibility across devices. Key features include:

## Interactive Scenarios: Simulations of real-world cyberattacks (e.g., phishing emails, ransomware alerts) that allow users to experience and learn from realistic attack scenarios.

## AI-Generated Questions: Dynamic questions tailored to the user’s progress, providing personalized feedback and reinforcement.

## Gamified Elements: Incorporation of points, badges, and leaderboards to promote engagement and sustained participation.

## Customizable Levels: Offering multiple modes—Beginner, Intermediate, and Expert—to cater to varying levels of cybersecurity knowledge.

# Project Planning

## Constraints

1. **Budget Constraints:** Limited funding may impact the breadth and depth of features available in early iterations.
2. **Schedule Constraints:** The incremental development approach requires careful time management across multiple phases.
3. **Technical Constraints:** The integration of AI APIs and the creation of realistic cyberattack simulations pose significant technical challenges.

## Project Issues

1. **Integration Complexity:** Merging AI-driven content with interactive simulations may require extensive testing and iterative refinement.
2. **Adaptability:** Keeping the game updated with evolving cybersecurity threats necessitates ongoing adjustments.
3. **User Feedback:** Gathering and integrating continuous feedback from diverse user groups (individuals, organizations, and educators) is critical but challenging.

## Team Members Tasks

Manager

Designer

Developper

## Ethical Issues

## Data Privacy: Ensure that all user data is securely handled and stored, complying with relevant data protection regulations.

## Content Accuracy: Maintain a high standard of content quality to avoid the dissemination of incorrect or outdated cybersecurity information.

## Inclusivity: Design the tool to be accessible and usable by a diverse range of users, irrespective of their technical expertise or background.

## Software Model Process:

## The project team evaluated several software development models before choosing the most appropriate approach. The models considered were:

## Waterfall: *Pros:*

## Easy to understand and manage

## Works well for projects with well-defined requirements *Cons:*

## Not adaptable to changing requirements

## Testing occurs late in the process, increasing risk

## Incremental: *Pros:*

## Flexible and adaptable to changes

## Allows customer feedback after each iteration

## Suitable for large, complex projects by breaking them into manageable pieces *Cons:*

## Potentially higher overall cost due to iterative development

## Requires significant customer involvement

## Re-use: *Pros:*

## Saves time by leveraging pre-built components

## Reduces repetitive development efforts *Cons:*

## Risk of higher maintenance if reused components become outdated

## May limit originality in design.

## Chosen Approach: “Incremental Development”

## Given the need to integrate dynamic AI-generated content and realistic cyberattack simulations, the incremental development model was selected. This approach provides the necessary flexibility to incorporate ongoing feedback and adapt to evolving cybersecurity threats, while also allowing parallel development of different features.

## 

## Feasibility Study:

## A comprehensive feasibility study was conducted to assess the viability of the project:

## Technical Feasibility: The project relies on integrating AI APIs and simulating real-world cyberattack scenarios. Modern web frameworks, cloud hosting, and scalable databases support these requirements, making the project technically feasible.

## Operational Feasibility: The interactive game addresses a clear need for improved cybersecurity awareness among individuals, organizations, and educational institutions. Its gamified design and adaptive learning approach ensure high user engagement and practical applicability.

## Financial Feasibility: While budget constraints may limit early iterations, the incremental release model allows for phased development. This minimizes upfront costs and supports iterative funding based on early successes and user feedback.

## Schedule Feasibility: Dividing the project into manageable iterations enables continuous progress and regular assessment, ensuring the project can be completed within a realistic timeframe despite the complexity of its features.

## 

## Tools/Technology:

## The project will leverage a suite of modern tools and technologies to ensure a robust and scalable solution:

## Front-end:

## Web technologies such as HTML, CSS, and JavaScript frameworks (e.g., React or Angular) for a responsive and intuitive user interface.

## Back-end:

## Node.js or a similar server-side platform to handle application logic and API integration.

## RESTful APIs for integrating AI-generated question modules and other dynamic content.

## Database:

## A scalable database system (e.g., PostgreSQL or MongoDB) for securely storing user profiles, progress data, and performance metrics.

## Cloud Services:

## Cloud hosting platforms (e.g., AWS, Azure, or Google Cloud) to ensure high availability, scalability, and performance.

## Development Tools:

## Version control (Git), continuous integration/continuous deployment (CI/CD) pipelines, and automated testing frameworks to support an agile development process.

## Standards:

## To ensure quality and consistency throughout the project, the following standards will be adhered to:

## Coding Standards:

## Use of industry-standard coding practices and documentation for maintainability.

## Security Standards:

## Implementation of robust security measures to protect user data and prevent cyber threats. Compliance with data protection regulations (e.g., GDPR) where applicable.

## User Interface & Accessibility:

## Adherence to UI/UX best practices and accessibility guidelines (WCAG 2.1) to make the game usable by a diverse audience.

## Process Standards:

## Adoption of Agile methodologies and Extreme Programming (XP) principles to facilitate continuous improvement and high-quality delivery.

## 

## Milestones:

## The project’s progress will be monitored through clearly defined milestones:

## Prototype Development:

## Create a basic simulation module for cyberattack scenarios.

## Integrate initial AI-generated question functionality.

## MVP (Minimum Viable Product) Release:

## Deploy core features including a tutorial, basic phishing and ransomware scenarios, and progress tracking.

## Gather initial user feedback to refine the system.

## Feature Expansion:

## Implement additional attack scenarios, intermediate/expert levels, and enhanced gamified elements such as points, badges, and leaderboards.

## Introduce corporate training modules with analytics and reporting features.

## Final Release:

## Complete integration of all planned features.

## Conduct thorough testing, finalize documentation, and prepare for full-scale deployment.

## Launch the final product with ongoing support and iterative updates based on user feedback.

# Requirements

## Use Cases

This section begins to describe in more specific and precise detail exactly what steps the system takes in the course of its performance. Use cases serve not only to more specifically define the system (and its boundaries), but also to identify functional requirements, to identify initial objects / classes, and to organize the work.

## Functional Requirements

## Data Requirements

## Non-Functional Requirements

Performance Requirements

Dependability Requirements

Maintainability and Supportability Requirements

Security Requirements

Usability and Humanity Requirements

Look and Feel Requirements

Operational and Environmental Requirements

Cultural and Political Requirements

Legal Requirements

# Design

## Class Diagrams

## Dynamic Model

## Subsystem Decomposition

## Hardware / software mapping

## User Interface

# Test Plans

Features to be tested / not to be tested

Pass/Fail Criteria

Approach

Suspension and resumption

Testing materials (hardware / software requirements)

Test cases

Testing schedule

# Implementation

Output

# Results Evaluation

# Conclusion

## Summary

## Novelty

## Integrity and Values

## Future Work

# References / Bibliography

: Cite all ideas, concepts, text, data that are not your own. If you make a statement, back it up with your own data or a reference. All references cited in the text must be listed. There are two main ways to cite a reference within a text:

Citing the reference by author’s name: the author’s name must be placed at the end of the sentence that is taken from that reference along with the year of publication, then in the reference section the author’s name is to be arranged in alphabetical order.

Citing the reference by numbers: you should start numbering from 1 and continue according to order of appearance in text. Numbers should be placed the end of the sentence that is taken from that reference, then in the reference section you start your reference list from number 1.

You are recommended to use the APA writing style, which cites the reference by the author’s name, in your references’ citations.

The first line of each entry in your reference list should be on the left margin. Subsequent lines should be indented five spaces from the margin. All references should be double-spaced. Capitalize only the first word of a title or subtitle of a work. Italicize titles of books and journals. Note that the italicizing in these entries often continues

beneath commas and periods. Each entry is separated from the next by a double space (thus the entire reference list is double spaced, with no extra returns added).

Authors' names are inverted (last name first); give last name and initials for all authors of a particular work. Your reference list should be alphabetized by authors' last names. If you have more than one work by a particular author, order them by publication date, oldest to newest (thus a 1991 article would appear before a 1996 article). When an author appears as a sole author and as the first author of a group, list the one-author entries first. If no author is given for a particular source, alphabetize by the title of the piece and use a shortened version of the title for parenthetical citations. Use "&" instead of “and” on the reference page and only within parentheses when citing multiple authors of a single work in your text. At the end of the project list all references cited in the text in alphabetical order.

For an article in a journal:

***Author, A. A., Author, B. B., & Author, C. C. (Year of Publication). Title of article. Title of periodical, Volume Number, pages.***

Example 1: Harlow, H. F. (1983). Fundamentals for preparing psychology journal articles. Journal of Comparative and Physiological Psychology, 55, 893-896.

Example 2: Kernis, M. H., Cornell, D. P., Sun, C. R., Berry, A., & Harlow, T. (1993). There's more to self-esteem than whether it is high or low: The importance of stability of self-esteem. Journal of Personality and Social Psychology, 65, 1190-1204.

For a chapter in a book:

***Author, A. A., & Author, B. B. (Year of Publication). Title of chapter. In A. Editor &***

B. Editor (Eds.), Title of book (pages of chapter). Location: Publisher. When you list the pages of the chapter or essay in parentheses after the book title, use "pp." before the numbers: (pp. 1-21).

Example: O'Neil, J. M., & Egan, J. (1992). Men's and women's gender role journeys: Metaphor for healing, transition, and transformation. In B. R. Wainrib (Ed.), Gender issues across the life cycle (pp. 107-123). New York: Springer.

For a web page:

***Author, A. A., & Author, B. B. (Date of Publication or Revision). Title of full work [online]. Retrieved month, day, year, from source Web site: URL.***

Example: Chou, L., McClintock, R., Moretti, F. & Nix, D. H. (1993.) Technology and education: New wine in new bottles: Choosing pasts and imagining educational futures. Retrieved August 24, 2000, from Columbia University Institute for Learning Technologies Web site: <http://www.ilt.columbia.edu/publications/papers/newwine1.html>

For an online journal:

***Author, A. A., & Author, B. B. (Date of Publication). Title of article. Title of periodical, xx, xxx-xxx. Retrieved month, day, year, from URL.***

Example: Frederickson, B. L. (2000, March 7). Cultivating positive emotions to optimize health and well-being. Prevention &Treatment, 3 Article 001a. Retrieved November 20, 2000, from <http://journals.apa.org/prevention/volume3/pre0030001a.html>

# Appendix

Glossary

Naming Conventions and Definitions

Code and links

User Manual