Interactive Web Application for Teaching Cybersecurity

A Comprehensive Platform for Beginners Across All Age Groups

FLORIDA TECH
FLORIDA'S STEM UNIVERSITY

Introduction

- Cybersecurity is a critical skill in the digital age.
- This web application provides an engaging and interactive platform designed to teach cybersecurity concepts to beginners of all ages.

Target Audience

- Children (ages 8-12): Fun games and simplified cybersecurity concepts.
- Teenagers (ages 13-18): Hands-on activities and real-world scenarios.
- Adults: Comprehensive tutorials and practical applications.
- Professionals: Advanced modules for upskilling.

Features of the Web Application

- Interactive tutorials and quizzes.
- Age-appropriate modules with gamification.
- Real-world cybersecurity challenges.
- Progress tracking and certifications.
- Support for multiple languages.

Teaching Modules

- Cybersecurity Basics: Introduction to cyber threats and protection.
- Digital Hygiene: Password security and safe online behavior.
- Hands-on Labs: Simulations of phishing attacks and malware analysis.
- Advanced Topics: Encryption, network security, and ethical hacking.

Benefits of the Platform

- Engages learners with interactive content.
- Customizes learning paths for different age groups.
- Bridges the gap between theory and practical skills.
- Promotes awareness and resilience against cyber threats.

- Some Interractive game methodologies planned

Image from
https://pixabay.com/illustrations/ai-generated-computer-hacker-8136170/

Example

- **Game Concept: Cyber Defender Quest**
- **Objective:** Players protect their virtual city from cyber threats by identifying, mitigating, and preventing cyberattacks through interactive challenges.

GAME 1:Cyber Defender Quest

Game Levels	Level 1: Spot the Phishing Attempt	Level 2: Password Fortress	Level 3: Malware Maze	Level 4: Two-Factor Savior	Level 5: Safe Browsing Adventure
	• Scenario: Players receive simulated emails with suspicious links or attachments. • Task: Identify phishing emails by looking for red flags like poor grammar, fake URLs, or urgent requests. • Reward: Earn shields to protect the virtual city.	• Scenario: Players create strong passwords for various accounts. • Task: Use given rules (e.g., length, special characters, no dictionary words) to generate passwords. • Bonus: Educate about password managers. • Reward: Secure accounts earn keys to unlock more features.	• Scenario: A malware file is hiding in a list of downloads. • Task: Identify the suspicious file based on its size, type, and origin. • Reward: Earn antivirus upgrades for the city.	• Scenario: Simulated login attempts require 2FA authentication. • Task: Select the correct 2FA method (e.g., email, app-based codes) to secure the account. • Reward: Strengthen defenses against future breaches.	• Scenario: Players navigate a virtual browser and encounter fake websites and legitimate ones. • Task: Identify safe sites by checking for HTTPS, secure certificates, and domain names. • Reward: Enhance the safety level of the city.

- **Game Concept: Cyber Decryptor**
- **Objective:** Players become virtual cybersecurity experts tasked with solving challenges by reverse-engineering software, malware, or encrypted data to uncover hidden secrets.

Image :https://pixabay.com/illustrations/hacker-hacking-cyber-security-hack-1944688/

Game 2: Cyber Decryptor

Game Levels

Level 1: Binary Explorer

- **Scenario:** Players are given a simple executable file.
- **Task:** Use a virtual disassembler to identify patterns, instructions, or unused code.
- **Learning Objective:** Understand how to analyze assembly instructions and basic binary files.
- **Reward:** Earn a key to unlock the next level.

Level 2: Cracking the Code

- **Scenario:** A mysterious software has hidden functions protected by basic password encryption.
- **Task:** Reverse engineer the program to find the hardcoded password and unlock the hidden function.
- **Learning Objective:** Learn to identify hardcoded data in binaries and understand simple cracking techniques.
- **Reward:** Earn decryption tools for future challenges.

Level 3: Malware Dissector

- **Scenario:** Players receive a simulated malware sample affecting a virtual machine.
- **Task:** Analyze the malware's behavior, identify the affected files, and reverse-engineer the malicious code to neutralize the threat.
- **Learning Objective:** Explore static and dynamic analysis techniques and learn malware behavior patterns.
- **Reward:** Build a malware analysis toolkit for later levels.

Level 4: API Analyzer

- **Scenario:** A program communicates with a hidden server.
- **Task:** Reverse-engineer the program to understand the API calls and manipulate the data being sent or received.
- **Learning Objective:** Learn about API interception and the importance of secure communication.
- **Reward:** Gain access to hidden developer tools.

Level 5: Capture the Exploit

- **Scenario:** A binary file contains a security vulnerability.
- **Task:** Reverse engineer the file to identify the vulnerability and exploit it to gain access to a protected system.
- **Learning Objective:** Learn about memory corruption, buffer overflows, and vulnerability exploitation.
- **Reward:** Unlock an advanced debugger to analyze complex binaries.