RMIT Hackathon 2025 – GenAI & Cyber Security

Application Report
CyberSafe: Stay Secure Online

Team Racer:
S3998345 – An Huynh Mai Thien
S4059598 – Cong Nguyen Phan
S4024618 – Do Bao Minh Khuong

Table of Contents

Introduction

In today's digital world, we are more connected than ever. But with this connection comes a growing risk. Australians are facing more cyber threats every day, from scams and phishing emails to serious data breaches in schools, workplaces, and homes. A cybercrime is reported every six minutes, yet many of us still do not know how to stay safe online.

That is where **CyberSafe** comes in. CyberSafe is an educational game that helps us learn how to protect ourselves in the digital world. It is designed for everyone, whether you are a student, a professional, or just someone who uses the internet regularly.

The game places us in real-life situations where we face online challenges and make choices that affect our progress and security. As we play, we learn how to spot threats like identity theft, unsafe websites, and suspicious messages, all while building better habits in a fun and interactive way.

CyberSafe is more than just a game. It is a simple and engaging way to build the skills we all need to stay safe online and take control of our digital lives.

Game Themes

CyberSafe focuses on three characters: a university student, an office worker, and a person at home. These roles were chosen because they face common cyber threats in real life. Each one helps us learn about different risks we might see in our own day-to-day activities.

University students often deal with phishing emails and stolen passwords. Many Australian universities are at risk of email fraud, and some have already had serious data breaches. In some cases, attackers have posted student data on the dark web [1]. Ransomware has also shut down school systems and caused major problems [2]. The student character helps players understand how to protect accounts, avoid fake emails, and stay safe online during study and campus life.

Office workers face threats like fake emails, password leaks, and unsafe remote work habits. Some workers use the same password across systems or ignore security steps [3]. Public Wi-Fi and personal devices also increase the chance of attacks. Criminals often trick people through phone calls, emails, or fake support messages [4]. The office character teaches players how to spot these risks, protect company data, and build stronger habits at work.

People at home are targets for scams, identity theft, and fake shopping websites. Scam losses in Australia reached over 170 million dollars in the first half of 2025 [5]. Many households also use smart devices that can be hacked or misused [6]. These risks affect families, older Australians, and young users alike. The home character helps players explore how to stay safe when shopping online, using apps, or managing personal information.

These three characters face different, real threats that have already affected many Australians. CyberSafe uses their stories to help us all understand what to watch for and how to stay safe online. Learning through these roles makes the game more personal, useful, and easy to follow.

Potential Impact

We designed CyberSafe for university students, office workers, and people at home because these groups face many cyber risks every day. Each group deals with different online threats and the game helps them learn how to recognize and avoid scams, phishing, and other attacks that could affect their personal or work lives.

Playing the game helps you build important skills like spotting fake emails and thinking carefully before clicking links or sharing information. We give rewards for safe choices and show what happens when you take risks, so you learn good habits that protect you online. These skills do not just help while playing but also make a real difference in your everyday digital life.

As you get better at staying safe online you also help those around you. Sharing what you learn can protect your family, friends, and coworkers from cybercrime. For workplaces this means fewer data breaches and stronger security overall. CyberSafe helps all of us build a

Technology Stack

- HTML
- Tailwind CSS
- JavaScript (ES6+)
- JSON
- GitHub Copilot (AI-assisted development)

Game Mechanics

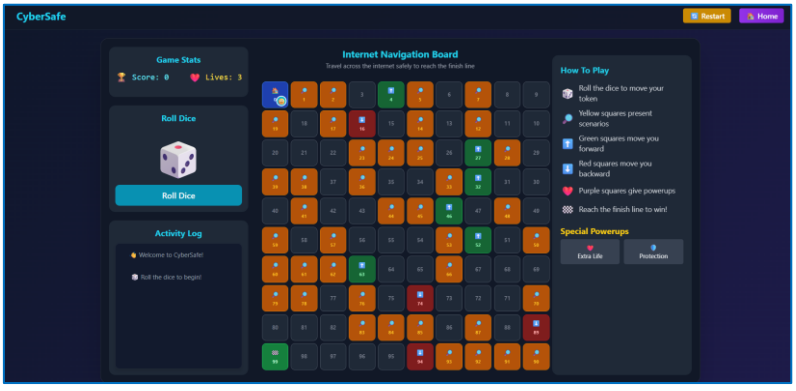

Image 1: Main Screen

The core gameplay is based on board progression and scenario response, where players move across tiles and answer cyber threat questions based on real-world examples.

Core Loop

- Roll a 3D dice (1–6) with animation and sound
- Move player token across the board
- Landing on tiles triggers effects based on tile color:
  - **Yellow (Scenario):** Present question card, answer wrong will deduct 1 heart
  - **Green (Forward):** Move ahead 2–4 tiles
  - **Red (Backward):** Move back 2–3 tiles
  - **Purple (Powerup):** Gain shield or extra life
  - **Empty:** No action taken
- Continue rolling or end game if win/lose conditions met
- **Scoring System**
  - Base points: Difficulty level × 2
  - Streak bonus: +25% per correct answer (up to 50%)
  - Movement bonus: +1 point per tile crossed
  - Win condition: Reach square 99
  - Loss condition: Life counter reaches 0

Learn Mode

Learn Mode is a non-gamified section designed for players who want to review educational content without gameplay pressure. It supports different learning styles and helps players prepare or review content before or after the challenge mode.

- **Features**
  - Browse all 60 scenarios
  - Filter by persona (Student, Office, Home) and difficulty (1–3 stars)
  - View scenario text, correct answer, and explanation
  - Navigate with arrows or search by keyword
  - Print-friendly formatting for offline study
  - No scoring, timers, or gameplay mechanics

Reflection

While developing CyberSafe, we learned a lot about how to make cybersecurity education both fun and meaningful. Our main challenge was making sure the game stayed enjoyable without making serious topics feel less important. Using a board game style with real-life roles like students, office workers, and home users helped players connect with the scenarios. Each group could see themselves in the situations, which made the learning feel more relevant.

We chose to build the game using plain JavaScript and store content in simple files. This made the game lightweight, easy to update, and accessible on most devices. It also allowed educators

to add or change scenarios without needing technical help. The Learn Mode gave players a way to study at their own pace, while the in-game feedback helped them learn from their choices. We focused on creating a safe and supportive space where players could make mistakes and try again.

Looking ahead, we see many ways to improve CyberSafe. We could add multiplayer features, adjust difficulty levels, and make the game available offline. Because of its simple design, CyberSafe can be used in classrooms, offices, and community programs. We believe it has strong potential to help more people learn how to stay safe in the digital world.

Reference

[1] Australian Cyber Security Centre, *"Annual Cyber Threat Report 2024–2025,"* Cyber.gov.au, 2025. [Online]. Available: https://www.cyber.gov.au/resources-business-andgovernment/reports-and-statistics/annual-cyber-threat-report-2024-25. [Accessed: Oct. 20, 2025].

[2] UQ SchoolsNet, *"Newcastle Grammar School post-mortem of ransomware infection,"* 2025. [Online]. Available: https://schoolsnet.uq.edu.au/news/newcastle-grammar-school-ransomware-post-mortem. [Accessed: Oct. 20, 2025].

[3] SecurityBrief, *"60% of Aussies bypass cybersecurity rules,"* 2025. [Online]. Available: https://securitybrief.com.au/story/60-of-aussies-bypass-cybersecurity-rules. [Accessed: Oct. 20, 2025].

[4] ABC News, *"Inside the 'Trinity of Chaos' group of young hackers,"* 2025. [Online]. Available: https://www.abc.net.au/news/2025-09-xx/trinity-of-chaos-hacker-group-australia. [Accessed: Oct. 20, 2025].

[5] Australian Competition and Consumer Commission (ACCC), *"National Anti-Scam Centre media update on $173.8m losses,"* 2025. [Online]. Available: https://www.accc.gov.au/media-release/national-anti-scam-centre-update-174m-losses. [Accessed: Oct. 20, 2025].

[6] CyberCX, *"CyberCX warns on household internet-connected devices,"* 2025. [Online]. Available: https://www.cybercx.com.au/insights/household-iot-device-risks. [Accessed: Oct. 20, 2025].