

Gameathon Abstract Template

Students should submit an abstract (Max 10 Pages PPT or PDF) covering the following sections:

1. Title of the Application/Game and Team Details

Clear, concise, related to cybersecurity and gamification should be considered for the title of the application/game. Team name and names of members (max 4), email ID and college/university name as submitted during the registration.

2. Problem Overview

Briefly describe the cybersecurity awareness problem you are addressing (e.g., phishing, malware, AI-based cybercrimes, social engineering, poor password practices, etc.).

3. Target Users

Who will use this application/game (students, employees, public, specific age group, etc.) and why they need it.

4. Proposed Solution (Core Idea)

Overall concept of the application/game. Platform(s) planned: mobile, desktop, web (Android, Windows, Mac, Linux, etc.). How it will create awareness and teach safe online behaviors. How in-game mechanics (levels, points, badges, leaderboards, challenges, storylines, etc.) are integrated. How users will interact with real-world case studies and decision-based simulations. Key features of the application/game should also be highlighted. Any specific design for accessibility (screen-reader support, color-blind friendly design, language options, simple UI, etc.) can also be mentioned.

5. Technology Stack (High-Level)

Planned tools/technologies (game engines, frameworks, languages, cloud services, etc.).

6. Learning Outcomes

What users will learn after playing (e.g., recognize phishing emails, respond to suspicious links, protect confidential information, identify AI-generated scams).

7. Uniqueness and Impact

What makes your idea different from existing cybersecurity awareness tools. How it will effectively reduce users' vulnerability to cyberattacks.