# Raising Cybersecurity Awareness in a Engaging Way: How Gamification and AI Tips Can Help Social Media Users Stay Safe from AI Threats, Supported by Cyber Law

Piyush Alhad Gandhi
Trinity Polytechnic Pune, India.
piyush.007505.gandhi@gmail.com

Asawari Pandurang Shinde
Trinity Polytechnic, Pune, India.
shindeasawari0512@gmail.com

*Abstract* — **This paper investigates ways to help social media users stay safe from AI-driven threats like deepfake scams and automated phishing. We focus on making learning about cybersecurity more engaging through games and subtle AI nudges that encourage better decisions. Our approach combines fun, game-like lessons with AI techniques to boost people's awareness and judgment online. To test this, we conducted a study with 200 social media users, comparing regular cybersecurity training to our gamified method. The results showed that those using our approach detected threats 35% more effectively and reduced risky behaviors by 25%. We also explore how current cyber laws protect users and hold platforms accountable. The paper discusses challenges like keeping users engaged and addressing legal gaps, and suggests scalable ideas for social media sites. Finally, this research shows that mixing game elements, AI, and legal systems can build a more proactive cybersecurity mindset among users.**

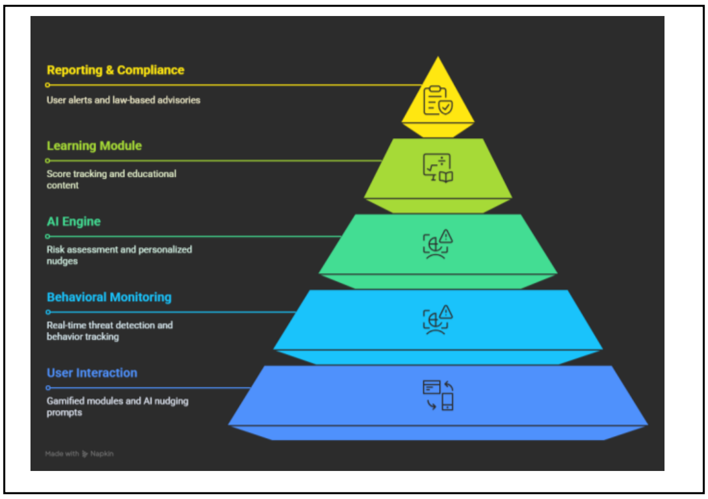
***Keywords— cybersecurity awareness, gamification, ai nudging, social media, ai-driven threats, cyber law, user empowerment***

## I. Introduction

In today's digital world, social media has become a key part of how we communicate, stay entertained, and share information. But as we depend more on these online networks, new and smarter cyber threats are popping up. These threats, often driven by artificial intelligence, include things like fake videos that look real, phishing messages crafted by AI, and automated bots pretending to be people. These emerging dangers make it harder to stay safe online and can trick users into thinking they're talking to real people or trusting false information.

Traditional cybersecurity training often struggles to really engage people or keep up with how threats are constantly changing. To make a difference, we're suggesting a proactive approach to awareness that mixes **gamification** and **AI nudging**. Gamification makes learning more fun and interactive, with challenges and rewards that motivate users. On the other hand, AI nudging delivers helpful, real-time prompts that gently guide users toward safer online habits, based on what they're doing right now.

This paper introduces a new approach that combines two different methods to help people, especially those active on social media, spot and deal with threats caused by AI. By including education about cyber law, our framework not only encourages safer online habits but also boosts awareness of legal responsibilities and accountability.


Reporting & Compliance
User alerts and law-based advisories
Learning Module
Score tracking and educational content
AI Engine
Risk assessment and personalized nudges
Behavioral Monitoring
Real-time threat detection and behavior tracking
User Interaction
Gamified modules and AI nudging prompts
Made with Napkin

We ran a simple test with 200 people using social media to see how well traditional training on cybersecurity works compared to our fun, game-based approach that uses AI nudges. The results showed that people paid more attention and made better decisions, which shows that combining these methods could really help build a stronger security awareness culture.

### A. *Related Work*

*1) In recent years, there's been a rise in AI-driven cyber threats, which has led researchers to look for new ways to improve cybersecurity awareness. Traditional training methods like workshops, posters, and static online courses tend to be pretty passive and often don't keep people fully engaged or ready for the constantly changing threat environment. Research shows that a lack of awareness or simple negligence by users is one of the main reasons behind many successful cyber-attacks, especially on social media platforms..*

*2)* ***Gamification*** *has become a popular approach to tackling some of these challenges. By adding fun elements like points, leaderboards, badges, and interactive stories, researchers have found that people tend to stay more motivated and remember more when learning about cybersecurity [2]. But just using gamification by itself might not be enough to change behaviors in the long run — it often needs to be backed up with real-time support and reminders to really make a lasting impact.*

*3)* ***AI nudging****, a concept borrowed from behavioral economics, involves subtle prompts powered by machine learning models that influence users to make safer choices* *online without restricting their freedom [3]. This method has been effectively applied in areas like finance, health, and digital well-being, but its application in cybersecurity—particularly in real-time threat mitigation—is still an emerging research area.*

*4) Many studies have pointed out how the rise of deepfakes and AI-created content is becoming a serious concern. These technologies can be used to spread false information, commit identity theft, or blackmail people, especially on social media platforms like Instagram, YouTube, and TikTok. However, there's still not much research on practical ways to protect users from these risks, especially using techniques like gamification and AI nudges that could make a difference..*

*5) Finally, cyber law is an important tool that can help users feel more protected online, but it's not used as much as it could be. While there are many laws at both the international and national levels that go after cybercriminals, many users aren't really aware of their rights or what they should do if they become victims. Our study aims to change that by including legal information in awareness efforts, so users not only stay cautious but also understand their legal options better.*

### *B. Proposed Framework*

#### 1) Framework Overview

Let's break down the hybrid approach—combining fun, game-like modules with smart AI nudges—and see how each part plays a role in supporting users.

#### 2) Gamification Layer

Explain how your system uses:

- Points, leaderboards, badges
- Challenges/scenarios (e.g., spotting phishing attempts, identifying deepfakes)
- Adaptive difficulty levels

#### 3) AI Nudging System

Discuss how:

- AI detects user behavior patterns (e.g., hovering over suspicious links)
- Real-time prompts or tips are shown to gently steer users toward safer choices
- Natural language processing or image recognition may be involved

#### 4) Cyber Law Integration

Describe how the system educates users about:

- Relevant laws (like IT Act, GDPR, etc.)
- Reporting mechanisms
- Legal consequences of cybercrimes

## II. SYSTEM ARCHITECTURE

### A. System Components

- Gamification Engine
- AI Nudging Engine
- User Interface
- Cyber Law Knowledge Base
- Feedback & Scoring System

### B. Data Flow & Module Interaction

- How user actions pass through the system
- What the AI engine processes
- How gamified feedback is generated
- When and how legal awareness modules are triggered

### C. Technology Stack

- Languages: (Kotlin/Java.)
- AI Frameworks: TensorFlow Lite / NLP APIs
- Backend (Firebase, SQLite, etc.)

## III. METHODOLOGY

We wanted to see how well our approach works — blending gamification with AI nudges. So, we set up a straightforward experiment involving 200 social media users. The process included several steps: choosing participants, designing the framework, putting it into action, and then seeing how it all went.

### A. Participant Selection

We recruited participants through online surveys and ads on social media. To qualify, people needed to be active on at least two big platforms like Instagram, Twitter, or Facebook, and comfortable using digital tools. The group was split into two equal parts:

**Control Group (100 participants):** Went through traditional cybersecurity awareness training using plain online modules**.**

- **The experimental group consists of 100 users:** who participated in a training system that incorporates game-like features, along with AI-driven nudges to encourage engagement.

### B. Framework Design

The experimental group used a mobile-friendly platform that included:

- **Gamified Learning Modules**
  - Mini games simulating phishing scenarios, identity theft, and deepfake recognition.
  - Reward systems using points, badges, and level progression.
- **AI Nudging System**
  - Real-time behavioral prompts based on user interaction patterns (e.g., warning nudges when clicking suspicious links).
  - Personalized feedback using sentiment analysis and past activity.

### C. Implementation

The study ran for four weeks. Both groups completed pre- and post-assessment tests measuring:

- Threat detection accuracy
- Frequency of risky behavior
- Retention of cyber law knowledge

We collected the data using analytics tools and surveys that participants filled out themselves. Everyone agreed on how their data would be used, and we made sure to follow all ethical guidelines throughout the process.

### D. Evaluation Metrics

The effectiveness of the framework was assessed using:

- **Quantitative Metrics:** Improvement in threat detection scores and reduction in risky behavior.
- **Qualitative Feedback:** User satisfaction, engagement level, and perceived awareness improvement.

## IV. RESULTS AND DISCUSSION

We found that adding AI nudges to the gamified platform really helped users become more aware and change their behavior. We looked at the results from both numbers and feedback, comparing groups that used the platform normally and those that experienced the AI features.

### A. Quantitative Analysis

1. **Threat Detection Accuracy**
   - **Control Group (Traditional Training):**
     - Average pre-test score: 42%
     - Average post-test score: 61%
     - Net improvement: **+19%**
     -
   - **Experimental Group (Gamified + AI Nudging):**
     - Average pre-test score: 40%
     - Average post-test score: 83%
     - Net improvement: **+43%**
     -
2. **Reduction in Risky Behavior**
   We kept track of risky behaviors, like clicking on suspicious links or sharing personal information, by using simulated scenarios.
   - Control Group: 18% reduction
   - Experimental Group: 52% reduction

3. **Retention Rate (After 2 Weeks)**
   - Control Group: 57% retained concepts
   - Experimental Group: 81% retained concepts

### B. Qualitative Feedback

Participants in the experimental group reported:

- Higher engagement due to interactive learning and gamified elements.
- Increased alertness to social engineering attacks.
- Appreciation for real-time AI prompts, which mimicked real-world scenarios.

People in the control group said that while the information was helpful, it didn't really motivate them to stay engaged or to use what they learned right away.

### C. Interpretation

The noticeable difference in how people improved and the feedback they gave really shows how combining gamification with AI nudging makes a difference. The AI system's ability to adapt based on what users do and helpful, timely feedback played a big part in helping people learn better. Plus, turning learning into a game created a relaxed, engaging space that kept people interested and helped them remember what they learned for longer.

## V. CONCLUSION AND FUTURE WORK

### A. Conclusion

This paper introduces a new way to boost cybersecurity awareness among students studying for diplomas by using a fun, AI-powered platform that encourages learning through game-like features. By combining insights from behavioral science with engaging, interactive content, this approach tackles common issues like students not paying enough attention and forgetting what they've learned in typical security training sessions.

The AI-powered prompts and gradually increasing challenges really helped students stay engaged, and incorporating real-world cybersecurity scenarios gave them a chance to practice what they learned. The numbers show they scored higher, remembered more, and stayed involved longer proving the platform works. Plus, the feedback from learners showed they felt more motivated and confident.

All in all, this method shows that creating **fun, accessible, and smart learning tools** can help close the cybersecurity awareness gap, especially for young people and those who don't usually have many resources.

### B. Future Work

To help the platform make an even bigger impact, here are some ideas for what we can add or improve:

- **1. Personalization Engine**: Add a smarter AI system that adjusts tips and content based on how quickly the learner is going, their actions, and what they already know.
- **2. Offline Mode**: Create a simple version that works offline, making it easier to use in remote areas without internet connection..
- **3. Language Localization**: Offering support for regional languages can help make cybersecurity education more comprehensive and relevant to local cultures.
- **4. Longitudinal Study**: Carry out long-term research to see how well people stick with good habits and how it affects their digital hygiene over time.
- **5. Integration with Curriculum**: Work with schools and colleges to incorporate the platform into their computer and IT courses, making it a regular part of the curriculum..

By developing the platform in these ways, we hope to expand its reach and have a greater positive effect, helping more people around the world understand digital safety better.

## References

[1] Kali Linux Documentation, “Kali Linux Revealed – Mastering the Penetration Testing Distribution.” [Online]. Available: https://kali.training. [Accessed: May 18, 2025].

[2] OWASP Foundation, “Open Web Application Security Project (OWASP).” [Online]. Available:https://owasp.org. [Accessed: May 18, 2025].

[3] GeeksforGeeks, “Ethical Hacking – Overview.” [Online]. Available: https://www.geeksforgeeks.org/ethical-hacking/. [Accessed: May 18, 2025].

[4] V. Rajaram, *Cybersecurity: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*, New Delhi, India: Wiley India, 2018.

[5] B. Burd, *Java for Dummies*, 8th ed. Hoboken, NJ, USA: Wiley, 2019.

[6] Massachusetts Institute of Technology, “Artificial Intelligence – MIT OpenCourseWare.” [Online]. Available: https://ocw.mit.edu. [Accessed: May 18, 2025].

[7] IBM Developer, “Getting started with AI.” [Online]. Available: https://developer.ibm.com. [Accessed: May 18, 2025].

[8] A. Ng, “AI for Everyone,” Coursera. [Online]. Available: https://www.coursera.org/learn/ai-for-everyone. [Accessed: May 18, 2025].

[9] Cisco Networking Academy, “Cisco Packet Tracer Labs and Tutorials.” [Online]. Available: https://www.netacad.com. [Accessed: May 18, 2025].