Leveraging Gamification and Game-based Learning in Cybersecurity Education: Engaging and Inspiring Non-Cyber Students

Dr Lowri Williams, Dr Eirini Anthi, Dr Yulia Cherdantseva, Dr Amir Javed

Cardiff University, Wales, UK

Introduction

- Cybersecurity is a critical field that requires comprehensive understanding and practical skills to counter potential threats.
- Traditional pedagogical methods include lectures, guided lab work (in technically safe environments), etc.
- However, they may not always engage and inspire learners effectively.

Gamification and Game-Based Learning

- By leveraging game elements into non-game contexts, gamification offers a promising tool for stimulating user engagement and promoting specific behaviours.

- Empirical research indicates that gamification in education leads to increased learner engagement, active participation, improved academic performance, and enhanced learning outcomes (Hamari et al., 2014).

Capture the Flag (CTF)

- Cybersecurity competition where participants engage in solving security-related challenges and tasks within a controlled environment.

- The primary aim is to identify and exploit vulnerabilities, thereby capturing "flags" which are often in the form of digital tokens, strings of text, or hidden files.

- Teams of players or individuals earn points for solving challenges across multiple categories (e.g. web security, cryptography, forensics, Open Source Intelligence (OSINT)

Limitations of Existing Capture the Flags (CTF)

- Technical difficulty: Novices and individuals without prior cybersecurity knowledge may find it difficult to access and engage with platforms effectively.

- Lack of accessibility: Some platforms target specific audiences, such as high school students or beginners, potentially leaving more advanced learners or those seeking deeper understanding underserved.

- Isolated challenges: Several platforms offer isolated challenges that do not provide learners with a clear understanding of how various cybersecurity concepts interrelate. This can hinder the development of a holistic cybersecurity skill set.

Limitations of Existing Capture the Flags (CTF)

- Emphasis on technical skills: Many platforms heavily emphasize technical skills and assume a solid foundation in cybersecurity. This can discourage beginners or individuals from non-technical fields from participating.

- Lack of comprehensive narrative: Some platforms lack a structured narrative that guides learners through the interconnectedness of cybersecurity aspects, resulting in a disjointed learning experience.

- Limited audience scope: Platforms are highly specialized, focusing on secure coding techniques and specific programming languages. This limited scope may not cater to individuals interested in broader cybersecurity topics.

Our Approach

- 2 styles of challenges
  - Open-Ended Capture the Flag
  - Story-Based Capture the Flag

Open-Ended Capture the Flag (CTF)

- Method:
  - Students are put in teams
  - Non-technical and open ended questions are provided
  - Students collaborate to answer questions
  - Solutions are submitted to teaching staff
  - Correct answers are awarded a ‘flag’ to input into the platform
  - Real-time score updates visible on a dashboard

Open-Ended Capture the Flag (CTF)

- Question examples:
  - *What method would you use to gain more information about the target before you actively start the exploitation?*
  - *Assuming as an attacker you have gained access to the organisation's network, what would you do next to gain more information about the IT infrastructure?*
  - *If you were to deploy a phishing attack, who would you target, and how would you deploy the attack?*

Open-Ended Capture the Flag (CTF)

- Promotes in class collaboration, critical thinking, and problem solving skills to address open-ended questions relevant to the cybersecurity domain.
- Provides structured guidance to help navigate the vast online cybersecurity information.
- Based on Vygotsky's (1978) educational theory, it emphasises supportive guidance in learning.
- Incorporates formative feedback through regular team check-ins.
  - Supported by Paul & Elder's (2001) theory for effective learning.
  - Enables real-time refinement of strategies & approaches.

Story-Based Capture the Flag (CTF)

- Themes around well-known events: Christmas, Easter, and generic themes.
- Narrative guided learning enhances task relevance.
- Suitable for remote, on-campus, or hybrid settings.
- Encourages team play (teams of four) or solo participation.
- Beginner-friendly challenges; no prior cybersecurity knowledge needed.

Story-Based Capture the Flag (CTF)

- Flags align with the overarching story, underscoring task relevance.
- Crafted hints guide without hindering critical thinking.
- Real-world cybersecurity scenarios within tasks, adding authenticity.

Example of a CTF Question

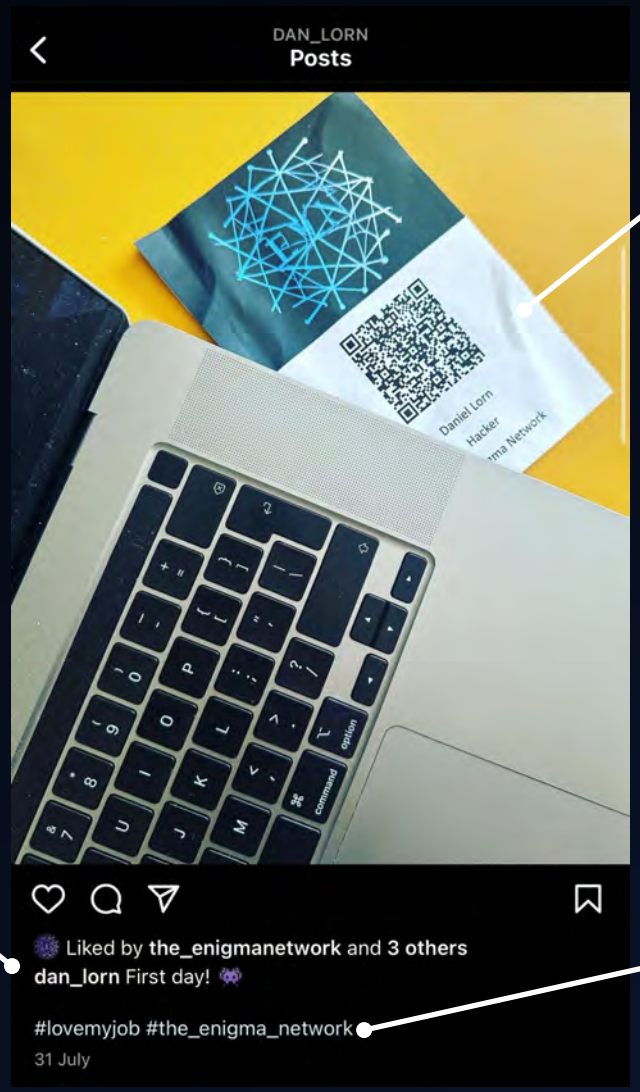
“In a dystopian future, an oppressive government entity known as The Enigma Network has taken control of the global internet infrastructure. They have implemented advanced surveillance techniques and censored free access to information.

A group of international open-source advocates, coders, and hackers have formed an underground collective called FreeNet.

As a member of this group, your goal is to systematically take down the Enigma Network's controls, liberating internet access.”

Q1 - Recon social media sites to see if you can find any useful information about The Enigma Network.

Example of a CTF Question



QR code

Employee name

Hashtag

Application and Feedback

- Feedback is gathered informally through tools like Mentimeter and Google Forms, offering first hand insights into the immediate reception and impact of the games, albeit without adhering to structured research assessment methodologies.
- Feedback has been very positive, endorsing its successful implementation.
- Participants have expressed enjoyment and have found it to be an effective learning environment.
- Collaborations with other universities have also been established, enhancing the diversity of participants and learning experiences.

Conclusions

- In our experience, gamification and game-based learning have shown great potential in enhancing cybersecurity education.
- By presenting innovative designs and successful implementations of these games, we hope to inspire further adoption and adaptation of such pedagogical strategies.
- This will contribute significantly to the evolution of cybersecurity pedagogy and create a more engaging and effective learning experience for learners.

Conclusions

- Additional structured research is still required - it is essential to quantify the effects of these gamified methods on the academic performance of students and investigate their adaptability across diverse disciplines.

- The games are not publicly available online to preserve their integrity and challenge, but educators or institutions can contact the corresponding author for arrangements to use them in their courses or events.

- Dr Lowri Williams - WilliamsL10@cardiff.ac.uk