Human Factors in Cybersecurity, Vol. 208, 2026, 31–41
https://doi.org/10.54941/ahfe1007410

Enhancing Cybersecurity Learning Through Online Platforms and Gamified Approaches

Dimitris Koutras[1], Kitty Kioskli[2], and Vangelis Malamas[1]

[1]Department of Informatics, University of Piraeus, 185 34 Piraeus, Greece
[2]trustilio B.V., Vijzelstraat 68, 1017 HL Amsterdam, The Netherlands

ABSTRACT

The way teaching used to be done in a lab, just doesn't show how important it is to be real, be lively, and think differently when it comes to modern security practice. As a result, the rise of online cybersecurity platforms, the use of challenge-based environments, and the use of game-based learning methods have all become powerful additions to traditional teaching methods. This paper looks at how well interactive methods work in teaching, by combining what the public knows, well-known learning theories, and what instructors have experienced in undergraduate and postgraduate cybersecurity courses. The present study looks at how online platforms, virtual training areas, gamified exercises and Capture-the-Flag (CTF) competitions can make people more interested, independent and able to learn. The research looks at how new technologies, like the Internet of Things (IoT) systems, blockchain infrastructures, and distributed cyber-physical environments, will affect the future of cybersecurity training. The paper ends with a blended learning framework and a research design for future real-world testing, emphasising the need to include practical digital ecosystems in today's cybersecurity courses.

Keywords: Cybersecurity education, Online learning platforms, Game-Based learning, Capture-the-Flag (CTF), Hands-on training

INTRODUCTION

Traditional learning environments, which rely on scripted laboratory exercises and static instructional materials, often fail to capture the dynamic, adversarial, and hands-on nature of real cybersecurity practice. As a result, universities and professional training centers have begun exploring new instructional approaches such as online cybersecurity platforms and game-based learning environments. Online platforms, including challenge-based laboratories and virtualized cyber ranges, provide students with opportunities to engage in realistic attack-defense scenarios while offering instructors scalable and secure environments for teaching. At the same time, game-based methodologies, such as cyber games, Capture-the- Flag (CTF) exercises, and interactive learning challenges, use core game mechanics to enhance engagement, motivation, and analytical thinking.

Received February 4, 2026; Revised April 9, 2026; Accepted April 24, 2026; Available online July 20, 2026

This paper aims to address these issues by presenting:

- an analytical exploration of the necessity and prospective effectiveness of online platforms and game-based methodologies in cybersecurity education,
- qualitative, experience-based insights derived from teaching cybersecurity courses at the University of Piraeus (UPRC),
- a proposed research design for future empirical investigation, and
- a practical framework for integrating these methods into university-level curricula.

This work does not present formal quantitative data. Instead, it synthesizes relevant concepts, teaching experience, and informal observations to construct a structured argument supporting the educational value of platform-based and game- based approaches in cybersecurity. A full empirical study is recommended as future work, which will benefit from the structured framework introduced in this paper.

Related Work

The latest research examines how technology can improve learning. These include online cybersecurity platforms, game-based learning methods, competitive challenge environments, and theoretical frameworks related to student motivation and experiential learning. So, this section explains the main ideas that have emerged from previous research and shows how gaps have emerged that made this study necessary.

A. Online Cybersecurity Platforms

Online cybersecurity platforms are now an important part of modern security education, as they provide students with safe, scalable, and realistic spaces to practice their offensive and defensive skills. Every building should have traditional computer labs. Virtualization should be used for their installation and updating. Online platforms allow thousands of students to use isolated challenge environments whenever they want, reset them immediately, and use them all at the same time.

One of the most popular platforms is Hack The Box (HTB). It is a web app of virtual machines that you can try out, courses that show you how to use them, and learning paths that are set up in steps. With HTB, users can do real penetration tests, like getting more privileges, attacking websites, reverse engineering, and more. TryHackMe (THM) is similar, making things easy to use and learn step by step. It has interactive spaces with instructions. The program utilizes a guided model, a feature that renders it particularly well-suited for novice users. However, it also incorporates advanced content, which is designed to facilitate the training of red and blue teams. Both HTB and THM are cloud-based. The virtual machines and sandboxes are automatically set up through browser-based interfaces, thereby relieving students of the responsibility of managing virtualization or network settings on their personal computers.

Online platforms also have significant educational benefits. Students receive immediate feedback on their actions, such as whether they were able to take advantage of a vulnerability or whether a configuration change reduced the likelihood of a threat. The latest studies look at the different ways technology can be used. Find out about learning environments and theoretical models related to students. Learning through doing and staying motivated. This section looks at the main approaches that have been identified in earlier research It also shows where there were gaps (Rehaimi et al., 2023).

B. Game-Based Learning in Cybersecurity

In contradistinction to conventional laboratory exercises, which characteristically adhere to a rigid, step-by-step structure, game-based environments are designed to encourage learners to explore, experiment and problem-solve in dynamic scenarios that emulate real attacker and defender behaviour. Game-based learning by Khan et al. (2022) is based on the integration of game mechanics, such as scoring systems, levels, hints, timers, achievements, and leaderboards, into cybersecurity tasks. These mechanics provide continuous feedback and clearly defined goals. They motivate students to engage with challenging tasks and to repeat them until mastery is achieved. Within educational settings, serious games are frequently employed to simulate realistic security incidents. According to Rajendran et al. (2025) These games may include activities such as analyzing suspicious network logs, locating the source of a breach, identifying misconfigurations, or defending against simulated attacks.

C. Capture-the-Flag (CTF) and Competitive Learning

The Capture-the-Flag (CTF) competitions according to Ken et al. (2025) and Beuran et al. (2025) are one of the most popular and well-known ways to learn cybersecurity. CTFs were first set up by hacker groups. They provide a set of technical challenges in a way that is similar to how hackers would actually attack or defend a system. Now, they are part of university courses, cybersecurity clubs, hackathons and national competitions. This shows that they are an important part of cybersecurity education. CTF competitions typically follow one of two models:

- Jeopardy-style CTFs, which present independent challenges in categories such as web exploitation, binary exploitation, digital forensics, steganography, cryptography, and reverse engineering. Students earn points by solving challenges in any order, allowing for flexible exploration and progress at their own pace.
- Attack-Defense CTFs, which simulate real network environments. Teams defend their own vulnerable systems while simultaneously attempting to attack others' systems. This type represents the real-world incident response, the vulnerability management, and the adversarial operations.

One of the main reasons CTFs are good for education is that they get students to use their knowledge in new ways, instead of just following instructions. CTF challenges are different from traditional labs. In traditional

labs, students usually just repeat the same commands. With CTF challenges, students have to explore, test their ideas and solve problems.

D. Engagement and Motivation in Technical Education

It is very important that students are interested and motivated in technical education, especially in cybersecurity. Research into education offers several useful theories and studies that can help us design and evaluate cybersecurity teaching (and, more generally, platform and game-based methods).

Importantly, Gao et al. (2024) mention some variable details concerning the Self-Determination Theory (SDT). According to this theory, there are three basic things that motivate people: autonomy, competence and relatedness. For example, a study looking at gamification and SDT found that "if gamification is used in the right way and is in line with SDT's framework, it can make learners more motivated".

In Yli et al. research is described a psychological state in which learners become fully immersed, find the challenge and skill balance optimal, and consequently experience deep engagement and high performance. In those "game" environ-ments, achieving the flow method is totally linked with the learning outcomes and the motivation.

An other state of motivation in combination with gamification according to Shettigar et al. (2025), Balalle et al. (2024), and Cigdem et al. (2024). Gamification is when you use game design elements (like points, badges and leaderboards) in situations that aren't games. It has been shown to increase engagement, motivation and sometimes academic performance. For example, one study found that students' attitudes towards gamification (using games in learning) were linked to how engaged they were in higher education. In the study of cybersecurity, platforms that use games and challenges are used to encourage people to practise, compete with others and gradually improve their skills. But designers must be careful to match these elements, because gamification that is not used in the right way can make people less motivated.

According to Ahmands definition (Ahmad et al., 2024), engagement is made up of different parts, including how a person acts, their feelings, and their thoughts. Research has shown that gamification has a different effect on these areas. For example, it can make people more active, but not necessarily more thoughtful. A recent review of research in this area concluded that strategies that use gamification in higher education still need to consider all the different ways to engage students holistically. This means that people teaching cybersecurity should not only look at how many students take part in challenges. They should also look at how much students learn, how they think, and whether they are still interested (Adeshola et al., 2024).

When we apply these theoretical ideas to cybersecurity teaching, we can see several important design priorities:

- Give students the freedom to choose their own challenges or roles (for example, attacker or defender).
- Work on getting better at something by doing more difficult tasks and getting help and support when you need it.

- Encourage students to work together by playing team-based games and having them collaborate with their peers.
- Look at how students are responding in different ways, like how they take part, how they think.

If we use these methods, we can greatly improve how motivated students are, how well they keep going, and how well they eventually learn cybersecurity skills.

Teaching Experience And Anecdotal Observations at University of Piraeus

The main ideas and the statistics in this work come from teaching experience at the University of Piraeus (UPRC), where cybersecurity is part of undergraduate and master's courses. Some formal data has been collected and in combination with informal observations and interactions in class, valuable insights are provided as you can see in Figure 1.

Another thing that people often say is that they like the tasks that are based on games. Students often suggest designing their own cyber games or taking part in challenges that are like games, like Capture the Flag events. Teacher observations also show the benefits of online platforms. They make it easier to set up, faster to grade and can be used in larger classes. Games, especially when played competitively or cooperatively as team activities, can make learning more fun and improve behaviour in the classroom.

Proposed Research Design for a Future Study

Micro-decisions don't happen in a space that is neutral. The way alternatives are shown, emphasized, delayed, or concealed in the interface affects how they look. (Trzaskowski et al. 2023) Even while users are typically expected to make quick decisions on privacy and security, the design of many digital interfaces actively pushes these decisions in certain directions. People often call these practices "dark patterns." They are design methods for interfaces that change how people engage by taking advantage of cognitive limits, habitual responses, and differences in attention.

To move forward, we need a well-planned study with real results. This chapter presents a research plan that will be used in future semesters. This will allow us to test the earlier hypotheses using real data.

A. Research Questions

The following research questions (RQs) are suggested:

- RQ1: How do students think online cybersecurity platforms compare to traditional lab exercises?
- RQ2: How much do game-based learning activities influence persistence and self-efficacy?
- RQ3: What is the best way to teach cybersecurity? Should we use different methods such as platforms, games, and lectures?

B. Methods and Research Design

This study outlines a plan for testing how well online cybersecurity platforms and game-based learning activities work compared to traditional lab classes. The methodology includes quantitative measurements, qualitative insights, and learning analytics from the platforms. The design examines both student performance and the depth of their learning across different teaching conditions.

Table 1: Comparison of instructional conditions.

Feature	Group A	Group B
Teaching Method	Lectures and scripted labs	Lectures with additional interactive activities
Online Platforms	Not used	Used for hands-on exercises
Game-Based Activities	None	Included (CTFs, challenges)
Learning Mode	Instructor-driven	Mixed: instructor + self-paced work
Hands-On Depth	Fixed lab steps	Realistic scenarios and challenges
Technology Interaction	Controlled lab en-vironment	Dynamic cyber ranges and online tools
Engagement Level	Moderate	High
Data Collected	Tests, questionnaires	Tests, questionnaires, analytics

Quantitative and Qualitative Components:

Quantitative Components

- Pre and post-learning conversations and assessments to see how much students have learned about topics such as vulnerability analysis, exploitation, and defensive configuration.

Qualitative Components

- Semi-structured interviews with volunteer students from each class to discuss their learning experience, challenges they faced, and what motivates them.
- Instructor notes collected throughout the study, documenting observations on student behaviour, group interactions, and differences across teaching approaches.

C. Experimental Design

A between-groups design will be used to compare the effectiveness of traditional and interactive teaching methods. Two instructional conditions will be examined:

Group A – Traditional Instruction

- Students receive traditional lectures and scripted lab exercises.
- No use of platform-based or game-driven tools.

Group B – Blended Interactive Instruction

- Students receive traditional instruction.
- Students also use online cybersecurity platforms, challenge-based environments, and game-based activities such as CTF-style tasks.

This design allows us to isolate the contribution of interactive tools and determine whether a blended approach leads to improvements in engagement, learning, and confidence.

D. Learning Analytics

When online platforms provide activity logs, learning analytics will be used to measure real-time behavioural indicators, including:

- Number of challenge attempts.
- Number of successfully completed challenges.
- Time spent on each activity.
- Speed of progression across learning modules.
- Frequency of retries and common error patterns.

These metrics provide objective insights into persistence, problem-solving approaches, and learning strategies. When combined with questionnaires and performance tests, they allow a richer analysis of student engagement and outcomes.

1) Modelling Trends: Regression analysis will be used to explore relationships between variables such as:

- student confidence,
- interest and engagement,
- time spent working,
- platform usage,
- and performance outcomes.

These models help identify which factors have the greatest influence on learning gains.

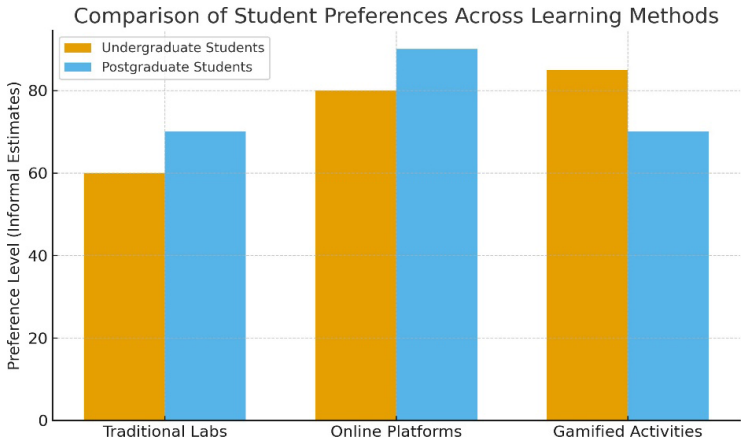

Figure 1: Overall statistics.

Impact to Lessons Planning

Based on the ideas in the plan and what we have learned from teaching, we can suggest several ways to include online platforms and game-based activities in cybersecurity courses.

A. The Structured Blended Learning Model

The model consists of three layers:

- Layer 1: Theory and Foundational Concepts

This layer focuses on the theoretical background and essential ideas. It is critical to establish the conceptual and technological basis needed for cybersecurity.

- Layer 2: Online Platforms for Practical Skill Development

This layer involves the use of online platforms that introduce realistic challenges. Students learn to exploit weaknesses, understand attack paths, and develop a system level perspective on cybersecurity tasks.

- Layer 3: Games for Engagement and Higher-Order Skills

This layer includes CTF competitions, scenario-driven games, and student-created game projects. These activities strengthen engagement, creativity, and advanced problem-solving skills.

This three-layer structure ensures that interactivity is used meaningfully and that the progression of learning is coherent pedagogically.

B. Things to Think About in Practice

- Scalability

Online platforms can be scaled up or down depending on class size. They reduce setup time and can be used effectively with large groups of learners.

- Training for Teachers

Instructors need to be familiar with these tools so they can monitor student progress, guide activities, and provide support when needed.

- Assessment

Platforms and games can be integrated into assessment through challenge completions, team performance, analytics, or reflective reports.

- Flexibility

Students benefit from environments where they can learn at their own pace. This is especially helpful for learners who enter cybersecurity courses with different levels of prior experience.

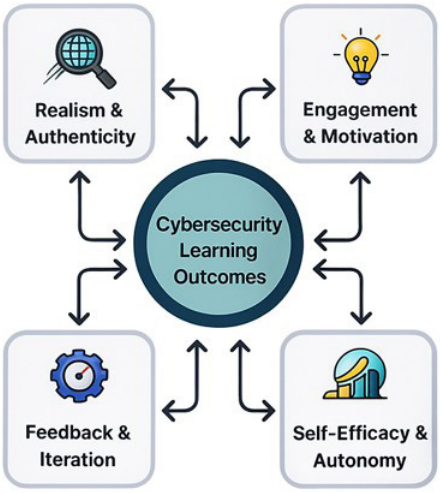

Figure 2: Learning outcomes.

Figure 3: Model.

CONCLUSION

These platforms have an influence that goes beyond traditional IT systems and now involves new technologies. As Internet of Things (IoT) devices becomes more common in homes, cities, healthcare (Koutras et al., 2024) and industry, we need to make sure that people learning about cybersecurity know about distributed sensing, embedded systems, real-time constraints and low power networking. Online ranges and gamified labs provide a safe space where IoT vulnerabilities (such as insecure protocols, exposed firmware, weak authentication, and supply- chain risks (Koutras et al., 2023)) can be explored without interacting with real-world infrastructure. Interactive challenges that simulate IoT botnets, smart-home attacks, or industrial IoT disruptions can prepare students for the new threat landscape shaped by cyber-physical interdependence. In the same way, blockchain.

(Malamas et al., 2023) and distributed ledger technologies bring new ways of making things decentralised, managing trust, and making sure data is secure. It is becoming more and more important for people who work in cybersecurity to understand problems with smart contracts, how people agree on things, the manipulation of tokens and reorganising chains. They can do this by playing around with blockchain labs, smart-contract challenges and cyber ranges that use blockchain. Future work will use information from past studies, controlled experiments, and learning-analytics models to check how training on a platform, game-driven scenarios, IoT experimentation, and blockchain security tasks can improve student performance.

ACKNOWLEDGMENT

The authors would like to acknowledge the financial support provided for the following projects: the 'Advanced Cybersecurity Awareness Ecosystem for SMEs' (NERO) project, which has received funding from the European Union's DEP programme under grant agreement No. 101127411.

REFERENCES

Adeshola, I., & Oluwajana, D. I. (2025). Assessing cybersecurity awareness among university students: Implications for educational interventions. Journal of Computers in Education, 12(4), 1283–1305.

Ahmad, Z., Sultana, A., & Siby, N. (2025). Building Research Capacity in Higher Education: Exploring Confidence as a Mediator of Contextual Support and Research Interest. Innovative Higher Education, 1–24.

Balalle, H. (2024). Exploring student engagement in technology-based education in relation to gamification, online/distance learning, and other factors: A systematic literature review. *Social Sciences & Humanities Open, 9,* 100870

Beuran, *R. (2025).* Capture the Flag Platforms. In *Cybersecurity Education and Training* (pp. 193–219). Singapore: Springer Nature Singapore.

Cigdem, H., Ozturk, M., Karabacak, Y., Atik, N., Gürkan, S., & Aldemir, M. H. (2024). Unlocking student engagement and achievement: The impact of leaderboard gamification in online formative assessment for engineering education. Education and Information Technologies, 29(18), 24835–24860.

Gao, F. (2024). Advancing gamification research and practice with three underexplored ideas in self-determination theory. TechTrends, 68(4), 661–671.

Ken, C. L., Juremi, J., Alizadeh, S., & Sulaiman, S. (2025, July). Enhancing Cybersecurity Education Through Gamified Learning and Capture the Flag (CTF) Platform. In *International Workshop on Learning Technology for Education Challenges* (pp. 69–82). Cham: Springer Nature Switzerland.

Khan, M. A., Merabet, A., Alkaabi, S., & Sayed, H. E. (2022). Game-based learning platform to enhance cybersecurity education. *Education and Information Technologies, 27*(4), 5153–5177.

Koutras, D., Dimitrakopoulos, G., Malamas, V., Kotzanikolaou, P., & Douligeris, C. (2024, December). Comparative Analysis and Implementation of HTTP3, MQTT, and CoAP for IoT Applications. In Proceedings of the 28th Pan-Hellenic Conference on Progress in Computing and Informatics (pp. 127–132).

Koutras, D., Malamas, V., Kotzanikolaou, P., & Dasaklis, T. (2023, January). A risk assessment methodology for supply chain tracking services. In 2023 International Conference On Cyber Management And Engineering (CyMaEn) (pp. 555–559). IEEE.

Malamas, V., Koutras, D., & Kotzanikolaou, P. (2023, November). Uninterrupted trust: Continuous authentication in blockchain-enhanced supply chains. In 2023 8th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM) (pp. 1–6). IEEE.

Rajendran, D. P. D., & Rangaraja, S. P. (2025). Game-based learning for cybersecurity: enterprise implications from testing competing theories involving immersion, cognitive load and autonomy. *Journal of Enterprise Information Management, 38*(3), 872–900.

Rehaimi, A., Sadqi, Y., & Maleh, Y. (2023, October). A comparative study of online cybersecurity training platforms. In *International Conference on Verification and Evaluation of Computer and Communication Systems* (pp. 122–134). Cham: Springer Nature Switzerland.

Shettigar, R., Kulkarni, N., Radhi, M. N. M., Batar, M. S., & Sheikh, S. (2025). Gamified learning through ICT: Transforming student engagement in the 21st Century. Advances in Consumer Research, 2(4), 1793–1802.