IOCMA 2026 Conference
The 2nd International Online Conference on Mathematics and Applications
10–12 June 2026 | Online
MDPI

Quantitative Modeling of Teen Cybersecurity Awareness in Gamified Learning

Esma Mustafa
Department of Mathematics, Faculty of Technology and Information, «Aleksandër Moisiu» University, Durrës, Albania

INTRODUCTION & AIM

Context:
Teenagers are increasingly exposed to cybersecurity risks.
Early awareness and education are critical to prepare them against digital threats.
To provide a strong foundation for strategy development in cybersecurity education.
To demonstrate how mathematical reasoning and gamification can enhance awareness and resilience among students.

Research Focus:Examines the interaction between students' cybersecurity awareness and quantitative mathematics modeling.Uses gamified teaching environments to make learning engaging and effective.

Methodological Approach:Applies statistical fundamentals, probability analysis, matrices, and logical algorithms.Builds mathematical models to measure sensitivity and preparedness against cyber threats.

Educational Perspective:Investigates how students perceive and apply computational thinking.Explores whether gamified cybersecurity education should be introduced earlier in school or primarily at the high school level.

Integration with AI:Combines mathematical logic with artificial intelligence to create interactive gamified environments.Encourages critical thinking, database analysis, and problem-solving skills

METHOD

Quantitative Modeling → Gamified Environment → AI Integration → Inclusive Design → Cybersecurity Awareness Outcome

Quantitative Modeling
Probability Analysis: students estimate likelihood of cyber risks and compare perceived vs. actual threats.

Matrices & Logical Algorithms: simulate decision-making processes in digital environments.Statistical Fundamentals: measure awareness levels, knowledge gaps, and sensitivity to cybersecurity issues.

Gamified Learning Environment
Cybersecurity scenarios transformed into **interactive challenges**.
Students earn points or rewards for identifying threats and applying mathematical reasoning.
Encourages **critical thinking, collaboration, and problem-solving**.

Integration with Artificial Intelligence
Adaptive Difficulty Levels: tasks adjust automatically depending on student performance.
Personalized Feedback: each learner receives tailored guidance to strengthen weak areas.
Inclusive

Pedagogical Design
Methodology is personalized by class level and student profile.Ensures participation of all students:Those with strong mathematical/computational skills.Those who struggle with abstract concepts.Activities are scaffolded, starting from simple interactive tasks to more complex modeling challenges.Promotes equity in learning, recognizing that cybersecurity awareness is a widespread phenomenon that must involve every student.

Unique Contribution
Combines quantitative modeling + gamification + AI + inclusivity into a single methodology.Provides a replicable framework for teachers to integrate cybersecurity awareness into mathematics, physics, and computer science curricula.Ensures that all students, regardless of ability level, can engage meaningfully with cybersecurity education.

RESULTS & DISCUSSION

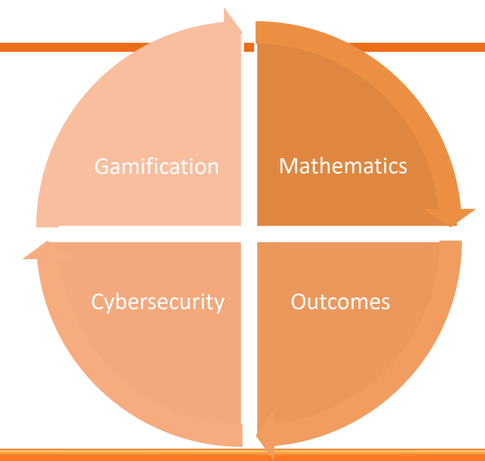
Student Engagement and Awareness The results indicate that students demonstrate significantly higher engagement when cybersecurity concepts are introduced through gamified learning environments. Interactive challenges and reward systems motivate learners to participate actively, while mathematical models provide measurable indicators of awareness. This shows that gamification transforms abstract concepts into practical experiences, making cybersecurity education more accessible to teenagers.

Knowledge Gains and Quantitative Outcomes The application of probability analysis, matrices, and logical algorithms allowed the study to quantify how students perceive and respond to cyber risks. Knowledge gains were evident across different student groups, with measurable improvements in their ability to identify threats and apply computational thinking. The discussion highlights that gamification acts as a multiplier effect: simple interactive tasks lead to substantial increases in understanding and retention.

Inclusivity and Differentiated Learning A key finding is that the methodology is inclusive. Students with strong mathematical skills and those who struggle with abstract reasoning both benefited from the personalized design of the gamified environment. Adaptive difficulty levels ensured that learners progressed at their own pace, while personalized feedback addressed individual weaknesses. This inclusivity is crucial, as cybersecurity awareness is a widespread phenomenon that must involve all students, regardless of ability level.

Pedagogical Value and Cross-Disciplinary Impact The integration of mathematics, computer science, and artificial intelligence created a cross-disciplinary learning ecosystem. Just as tourism impacts multiple sectors of the economy, this methodology impacts multiple areas of education: mathematics, informatics, logic, and critical thinking. The discussion emphasizes that gamification bridges the gap between theoretical modeling and practical application, offering a replicable framework for schools.

Resilience and Future Potential The adaptability of the gamified model demonstrates resilience against learning barriers. Students not only improved their cybersecurity awareness but also developed transferable skills such as problem-solving, collaboration, and critical thinking. This positions the methodology as a valuable contribution to modern curricula, with strong potential for expansion into other subjects and educational levels.



CONCLUSION

The study demonstrates that combining quantitative modeling, gamification, and artificial intelligencecreates an effective framework for teaching cybersecurity awareness to teenagers.
Results show that students not only improved their knowledge of cyber threats but also developed critical thinking, problem-solving, and collaborative skills.Overall, the thesis provides a strong foundation for future strategies in education, highlighting the importance of mathematical logic and gamified environmentsin preparing students for digital resilience.

FUTURE WORK / REFERENCES

1. Gee, J. P. (2007). What video games have to teach us about learning and literacy. Palgrave Macmillan.
2. Prensky, M. (2001). Digital game-based learning. McGraw-Hill.
3. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38(1), 97–102. https://doi.org/10.1016/j.cose.2013.04.004