Gaming to Cybersecurity: Enhancing Skills in High School Computer Science Students

Gullali Niazai

ORCID: http://orcid.org/0009-0005-6017-0452

Abstract

The rapid expansion of digital technology has increased the demand for individuals who possess strong cybersecurity knowledge, analytical ability, problem-solving capacity, adaptability, and ethical awareness. High school students studying computer science represent an important future source of cybersecurity talent; therefore, educational institutions need innovative methods for identifying and developing the skills that support cybersecurity learning. At the same time, video games have become a common part of the digital lives of many adolescents. Although gaming is frequently discussed in relation to entertainment and possible negative effects, it may also provide repeated opportunities for players to practice problem-solving, strategic planning, pattern recognition, persistence, collaboration, rapid decision-making, and adaptation. Several of these abilities may be relevant to computer science and cybersecurity education.

This research paper examines the extent to which video game playing habits can contribute to the development of cybersecurity-related skills among high school students studying computer science. The paper adopts a balanced and evidence-based position. It does not claim that playing commercial video games automatically produces cybersecurity expertise. Rather, it argues that certain forms of gaming may develop transferable cognitive, behavioral, and social abilities that can support cybersecurity learning when those abilities are deliberately connected with formal instruction, practical exercises, ethical guidance, and cybersecurity-specific learning environments.

The study proposes a mixed-method, quasi-experimental research design involving approximately 200 high school computer science students. Quantitative data may be collected through a gaming habits questionnaire, cybersecurity knowledge tests, practical skills assessments, logical reasoning tasks, and pre-test/post-test comparisons. Qualitative data may be obtained through classroom observation, student interviews, and teacher interviews. An experimental group would receive structured game-based cybersecurity learning activities in addition to conventional instruction, while a comparison group would receive the same core cybersecurity content through conventional approaches.

The paper concludes that balanced and purposeful gaming may provide a useful foundation for selected cybersecurity-related abilities, but educational benefits are likely to depend on the nature of the game, the intensity and quality of engagement, the learner's prior knowledge, and the presence of structured instruction and reflection. The strongest educational value is expected when game-based experiences are intentionally aligned with measurable cybersecurity learning outcomes.

Keywords

Video Games, Cybersecurity Education, High School Students, Computer Science Education, Serious Games, Gamification, Computational Thinking, Cybersecurity Skills, Game-Based Learning, Digital Education, Capture the Flag

1. Introduction

The twenty-first century has become deeply dependent on digital technology. Computers, smartphones, cloud platforms, online banking systems, educational networks, government services, healthcare systems, communication technologies, and business operations are increasingly interconnected. This dependence has created enormous opportunities for society, but it has also increased exposure to cyber threats. Phishing, malware, ransomware, social engineering, identity theft, unauthorized access, data breaches, and other forms of cybercrime demonstrate that digital security is no longer a specialized concern limited to information technology departments. Cybersecurity has become an important social, educational, economic, and national concern.

As cyber threats continue to evolve, the world requires people capable of understanding complex digital environments and responding intelligently to security problems. Cybersecurity professionals require technical knowledge, but knowledge alone is not enough. They also need the ability to investigate, recognize patterns, solve unfamiliar problems, make reasoned decisions, communicate with others, adapt to changing circumstances, and continue learning throughout their careers.

The question of how these abilities should be developed among young students is therefore increasingly important. Traditional instruction remains valuable, particularly for teaching theoretical foundations. However, cybersecurity is also a practical and problem-oriented discipline. Students often learn more deeply when they analyze scenarios, investigate evidence, test ideas, make decisions, receive feedback, and reflect on their mistakes.

This creates an opportunity to examine an activity that is already familiar to many young people: video gaming. Video games are frequently treated as entertainment. In some discussions, gaming is presented primarily as a source of distraction. Excessive gaming can indeed create problems, especially when it interferes with sleep, education, physical activity, family responsibilities, or social well-being. However, treating every form of gaming as identical ignores major differences between game genres and playing behaviors.

The central argument of this paper is that certain forms of balanced and purposeful video-game engagement may contribute to the development of transferable cognitive, behavioral, and collaborative abilities relevant to cybersecurity learning; however, these potential benefits become educationally meaningful primarily when they are intentionally connected with formal cybersecurity knowledge, practical assessment, ethical principles, and structured learning activities.

2. Background of the Study

Modern games can contain sophisticated narratives, realistic simulations, complex strategic systems, large virtual environments, multiplayer communication, problem-solving challenges, and interactive feedback systems. Players may be required to observe information, make predictions, test strategies, manage resources, coordinate with others, and adapt when circumstances change. These characteristics have encouraged educators to explore games as learning environments.

Interactive games commonly follow a cycle of challenge, analysis, decision, action, feedback, failure or success, reflection, and adaptation. This sequence has considerable relevance to computer science education. Programming frequently involves experimentation: a student writes code, executes it, observes the output,

identifies errors, modifies the solution, and tries again. Cybersecurity learning can follow a similar process through safe, authorized simulations.

The present study distinguishes between entertainment gaming, serious games, gamification, cybersecurity simulations, and capture-the-flag activities. Entertainment games are primarily designed for enjoyment. Serious games are designed with educational or training objectives. Gamification uses selected game elements such as points, levels, feedback, badges, or competition in activities that are not necessarily complete games. Cybersecurity simulations create realistic but controlled scenarios, while capture-the-flag activities present authorized technical and analytical challenges.

The research therefore asks not simply whether video games are beneficial or harmful, but which games, which skills, which students, under which educational conditions, and measured by which outcomes.

3. Statement of the Problem

Cybersecurity education requires students to develop a combination of technical knowledge and broader intellectual and behavioral abilities. Problem-solving, analytical reasoning, persistence, pattern recognition, decision-making, collaboration, and adaptability may all contribute to successful cybersecurity learning.

Many high school computer science students already participate in video gaming. However, schools generally possess limited evidence about whether particular forms of gaming are associated with useful cybersecurity-related competencies. Increased engagement should not automatically be interpreted as increased competence. Similarly, gaming duration alone may not indicate educational value. The relationship between video game playing habits and measurable cybersecurity-related skills among high school computer science students therefore remains insufficiently understood, particularly regarding which gaming experiences may produce transferable abilities and how those abilities can be intentionally connected with formal cybersecurity education.

4. Purpose of the Study

The purpose of this study is to investigate how video game playing habits may contribute to the development and enhancement of cybersecurity-related skills among high school students studying computer science. The study examines both naturally occurring gaming habits and the effect of a structured game-based cybersecurity learning intervention.

Specifically, the research aims to determine whether students' experience with different game genres is associated with selected skills relevant to cybersecurity and whether carefully designed game-based cybersecurity activities can improve measurable learning outcomes beyond conventional instruction alone.

5. Research Objectives

1. To identify common video game playing habits among high school computer science students.
2. To classify the major categories of games played by participating students.
3. To identify cognitive, behavioral, and collaborative abilities potentially developed through gaming.
4. To examine the relationship between gaming habits and logical problem-solving performance.
5. To investigate the relationship between selected gaming genres and pattern-recognition ability.
6. To examine whether strategic gaming experience is associated with strategic and risk-based decision-making.
7. To investigate whether cooperative gaming experience is associated with teamwork during cybersecurity activities.
8. To compare cybersecurity knowledge and practical performance among students with different gaming profiles.
9. To evaluate the effectiveness of a structured game-based cybersecurity learning intervention.

10. To examine student and teacher perceptions of the educational value of game-based cybersecurity learning.
11. To identify possible negative effects of excessive gaming on academic and personal functioning.
12. To develop recommendations for responsible integration of game-based learning into high school cybersecurity education.

6. Research Questions

1. What video game playing habits are most common among high school computer science students?
2. Which types of games are most frequently played by the students?
3. What cognitive and behavioral skills do students believe they develop through gaming?
4. Is there a statistically significant relationship between gaming habits and cybersecurity-related problem-solving ability?
5. Do students with greater experience in strategy and puzzle games perform differently on logical reasoning and pattern-recognition assessments?
6. Is cooperative multiplayer gaming associated with stronger performance in team-based cybersecurity exercises?
7. Do students who participate in structured game-based cybersecurity learning demonstrate greater improvement in cybersecurity knowledge than students receiving conventional instruction alone?
8. Do students who participate in structured game-based cybersecurity learning demonstrate greater improvement in practical cybersecurity performance?
9. How do students describe the role of failure, experimentation, feedback, and persistence in game-based learning?
10. What negative consequences do students and teachers associate with excessive or unbalanced gaming?
11. Which elements of game-based learning are most suitable for cybersecurity education at the high school level?

7. Research Hypotheses

H1: There is a statistically significant positive relationship between purposeful engagement with cognitively demanding video games and cybersecurity-related problem-solving performance among high school computer science students.

H2: Students who regularly play strategy and puzzle-based games demonstrate higher mean scores in logical reasoning and pattern-recognition tasks than students with little or no experience of such games.

H3: Students with regular experience in cooperative multiplayer games demonstrate stronger teamwork performance during structured group cybersecurity activities than students with limited cooperative gaming experience.

H4: Students receiving conventional cybersecurity instruction combined with structured game-based learning demonstrate significantly greater improvement in cybersecurity knowledge from pre-test to post-test than students receiving conventional instruction alone.

H5: Students receiving conventional cybersecurity instruction combined with structured game-based learning demonstrate significantly greater improvement in practical cybersecurity assessment performance than students receiving conventional instruction alone.

H6: Gaming duration alone is not a sufficient predictor of cybersecurity competence after factors such as prior computer science knowledge, prior cybersecurity exposure, and game genre are considered.

H7: Excessive and poorly regulated gaming is associated with negative self-reported effects on time management and academic responsibilities and does not necessarily correspond to improved cybersecurity performance.

8. Significance of the Study

This study is significant for students, teachers, schools, curriculum designers, researchers, and the wider cybersecurity education community. Students may discover that some skills developed through hobbies can have value when connected with formal learning. Teachers may use the findings to design more engaging and effective cybersecurity activities, including simulations, puzzles, team challenges, and authorized capture-the-flag exercises.

Schools may benefit from a better understanding of how students' existing digital interests can be connected with future-oriented education. Curriculum designers may use the findings to combine theoretical knowledge with interactive practice. For researchers, the study contributes to a developing field that requires stronger evidence about evaluation methods, learning outcomes, comparison groups, and long-term effectiveness.

9. Scope and Delimitations of the Study

The study focuses on high school students enrolled in computer science or closely related information technology courses. It examines gaming habits, selected game genres, cybersecurity knowledge, cybersecurity problem-solving, practical cybersecurity exercises in authorized environments, logical reasoning, pattern recognition, teamwork, and student perceptions.

The study does not attempt to determine whether gaming can independently produce professional-level cybersecurity expertise. It does not evaluate real-world unauthorized hacking. All practical activities must remain within legal and controlled educational environments. Because the proposed sample is limited to selected high schools, findings may not automatically generalize to all countries, age groups, or educational systems.

10. Operational Definitions

Video Game Playing Habit: The frequency, duration, genre preference, style, and pattern of an individual's engagement with digital games.

Purposeful Gaming: Gaming involving meaningful cognitive challenge, strategic planning, problem-solving, collaboration, simulation, or structured learning objectives.

Excessive Gaming: Gaming that interferes with important educational, personal, health, or social responsibilities.

Cybersecurity-Related Skills: Knowledge and abilities relevant to learning and practicing cybersecurity, including problem-solving, threat recognition, pattern recognition, logical reasoning, risk prioritization, secure decision-making, collaboration, and practical understanding of basic security concepts.

Serious Game: A game designed primarily or substantially to achieve objectives beyond entertainment, such as education, training, awareness, or skill development.

Gamification: The use of selected game elements, such as points, levels, feedback, badges, challenges, and leaderboards, in a non-game educational environment.

Game-Based Learning: The deliberate use of games or game structures as part of an educational process.

Capture the Flag: An authorized cybersecurity challenge environment in which participants solve technical or analytical tasks to discover hidden indicators or flags.

11. Literature Review

Game-based learning is supported by the principle that learners often understand concepts more deeply when they actively engage with problems rather than passively receive information. Interactive games commonly involve objectives, constraints, rules, feedback, challenge, and progression. These elements can create repeated learning cycles and encourage experimentation.

Research on educational games has reported generally positive potential for supporting computational thinking and programming concepts, while also emphasizing differences in study quality, game design, and evaluation methods. These findings are relevant because computational thinking overlaps with several foundational abilities useful in cybersecurity, including decomposition, abstraction, algorithmic reasoning, and systematic problem-solving.

The relationship between gaming and cognition is complex. Recent meta-analytic research has reported statistically significant but generally small associations between video-game play and several cognitive domains. This evidence does not justify the claim that every gamer becomes cognitively superior. Instead, it suggests that game genre, task demands, frequency, player characteristics, age, research design, and outcome measures all matter.

Strategy games may support habits such as considering alternatives, managing limited resources, anticipating consequences, and planning over multiple stages. Puzzle games frequently require players to identify relationships, infer rules, eliminate incorrect possibilities, and test hypotheses. These processes may be relevant to programming, debugging, digital forensics, log analysis, and incident investigation.

Pattern recognition is also important in cybersecurity. Analysts may need to identify repeated failed authentication attempts, unusual access times, abnormal network traffic, suspicious sequences of events, or similarities between fraudulent messages. Educational activities can make the connection explicit by asking students to compare normal and abnormal patterns and justify their conclusions.

Persistence is another potentially important characteristic. Games often normalize repeated attempts after failure. Computer science similarly requires productive failure through debugging and experimentation. A well-designed learning environment should provide meaningful feedback so that unsuccessful attempts become opportunities for improvement.

Cooperative multiplayer games may expose students to information sharing, role allocation, coordination, and rapid communication. However, educational teamwork must be assessed directly because gaming experience alone does not guarantee respectful or effective collaboration.

Cybersecurity serious games provide the strongest direct connection between gaming and cybersecurity education. Systematic reviews have identified a broad range of games addressing general cybersecurity awareness and more specialized topics such as ethical hacking and networking. The literature is promising but also highlights continuing limitations in game design, evaluation, target audiences, and evidence of training effectiveness.

A central lesson from the literature is that engagement is not identical to learning. Students may enjoy a game and still show limited improvement on objective assessments. The present study therefore proposes multidimensional evaluation of cognitive, practical, behavioral, collaborative, and affective outcomes.

12. Conceptual Framework

The proposed framework is based on transferable skill development.

Gaming Habits and Game Characteristics:
Challenge, complexity, puzzles, strategy, simulation, feedback, progression, teamwork, competition, exploration, and repeated attempts.

Potential Intermediate Skills:
Problem-solving, logical reasoning, pattern recognition, strategic thinking, persistence, adaptability, decision-making, communication, collaboration, and resource management.

Structured Educational Translation:
Computer science instruction, cybersecurity concepts, simulations, practical laboratories, authorized CTF activities, case studies, teacher feedback, and ethical reflection.

Cybersecurity Outcomes:
Cybersecurity knowledge, threat recognition, incident-response reasoning, risk prioritization, secure decision-making, practical problem-solving, teamwork, and ethical awareness.

The model is: Gaming Habits and Game Characteristics → Transferable Cognitive, Behavioral and Collaborative Skills → Structured Educational Translation → Measurable Cybersecurity Learning Outcomes.

The educational translation stage is essential. Without it, transfer from gaming to cybersecurity may remain weak or uncertain.

13. Research Methodology

The proposed study adopts a pragmatic mixed-method research orientation. Quantitative data are necessary to examine measurable relationships and differences, while qualitative data are necessary to understand students' experiences and perceptions.

The study uses a mixed-method quasi-experimental design with two interconnected components. The first is a comparative survey examining gaming habits alongside cybersecurity-related assessment performance. The second is a pre-test/post-test educational intervention in which an experimental group receives structured game-based cybersecurity activities in addition to conventional instruction, while a comparison group receives the same core cybersecurity content through conventional approaches.

The target population consists of high school students studying computer science or information technology, approximately 15 to 18 years of age. A proposed sample of approximately 200 students may be selected, subject to institutional access, ethical requirements, and statistical power considerations.

A multistage sampling procedure may be used: select participating schools, obtain institutional permission and required consent, recruit eligible students, collect baseline information, and assign or match students into experimental and comparison conditions where feasible.

14. Research Instruments

1. Demographic and Academic Questionnaire: age group, grade, computer science experience, programming experience, previous cybersecurity education, and access to digital technology.

2. Gaming Habits Questionnaire: frequency of play, weekly hours, platforms, preferred genres, strategy-game use, puzzle-game use, simulation-game use, cooperative multiplayer experience, programming or cybersecurity challenge experience, perceived benefits, and possible negative effects.

3. Cybersecurity Knowledge Test: phishing, social engineering, password security, authentication, multi-factor authentication, malware, ransomware, network-security fundamentals, digital privacy, public Wi-Fi risks, and basic incident response.

4. Practical Cybersecurity Assessment: safe and authorized tasks such as identifying phishing indicators in fictional emails, analyzing simplified authentication records, recognizing suspicious behavior in fictional logs, identifying risky password practices, prioritizing defensive actions, and identifying weaknesses in fictional scenarios.

5. Logical Reasoning and Pattern Recognition Test: non-cybersecurity tasks used to assess foundational reasoning separately from prior cybersecurity knowledge.

6. Teamwork Observation Rubric: information sharing, listening, role participation, respectful communication, evidence-based discussion, coordination, and contribution to group decisions.

7. Semi-Structured Interview Protocol: perceptions of gaming and problem-solving, learning through failure, similarities between gaming and cybersecurity, motivation, teamwork, and possible negative effects.

15. Validity and Reliability

Research instruments should be reviewed by cybersecurity educators, computer science teachers, educational researchers, and assessment specialists. Content validity can be strengthened by ensuring that assessment items represent intended cybersecurity learning objectives.

The questionnaire should undergo pilot testing. Reliability may be examined using appropriate internal consistency measures for multi-item scales. Practical assessments should use clear scoring rubrics. Where multiple evaluators assess observations or practical tasks, inter-rater consistency should also be considered.

16. Research Procedure

Phase 1: Preparation. Obtain institutional approval and ethical permission. Develop and review research instruments. Conduct a pilot study where appropriate.

Phase 2: Baseline Data Collection. Students complete demographic and gaming questionnaires, a cybersecurity knowledge pre-test, a practical baseline assessment, and a reasoning assessment.

Phase 3: Eight-Week Educational Intervention.

PHASE 3: EIGHT-WEEK EDUCATIONAL INTERVENTION

The educational intervention was implemented over a period of eight weeks. The experimental group received cybersecurity instruction through a structured game-based learning approach, while the comparison group received the same core cybersecurity content through conventional teaching methods without the additional structured game-based activities.

Week	Focus Area	Key Activities (Experimental Group)	Comparison Group
Week 1	Cybersecurity Foundations	• Introduction to cybersecurity basics • Digital threats and attack types • Ethics, authorization, and legal boundaries	Same core content delivered through traditional instruction (no game-based activities).
Week 2	Threat Analysis & Evidence Evaluation	• Puzzle-based challenges • Threat identification • Evidence collection and evaluation	Same core content and examples without structured puzzle activities.
Week 3	Phishing Challenge	• Identify phishing emails, links, and messages • Spot suspicious indicators • Interactive phishing simulation	Same core content and examples without phishing challenge.
Week 4	Password & Authentication Challenges	• Strong password creation • Password management • Multi-factor authentication practice	Same core content delivered through traditional instruction.
Week 5	Network & Anomaly Simulation	• Network security concepts • Anomaly detection exercises • Identify unusual activities in a simulation	Same core content and examples without network simulation.
Week 6	Team Incident-Response Exercise	• Team-based incident analysis • Investigate a simulated security incident • Develop and present response plan	Same core incident-response content through lecture/discussion only.
Week 7	CTF-Style Educational Challenge	• Authorized Capture-the-Flag (CTF) challenge • Apply skills in a safe environment • Solve security challenges in teams	Same core content without CTF-style challenge.
Week 8	Review, Assessment & Feedback	• Review of key concepts • Post-test and practical assessment • Student feedback and selected interviews	Same review and assessment without game-based activities.

This design allows comparison of learning outcomes between the game-based learning approach and the traditional instructional approach.

Figure 1: 8Week Plan

The comparison group receives the same core cybersecurity content without the additional structured game-based activities.

17. Data Analysis Plan

Descriptive statistics including frequency, percentage, mean, median, and standard deviation may describe gaming habits and student performance.

Correlation analysis may examine relationships between strategy-game engagement and logical reasoning, puzzle-game engagement and pattern recognition, cooperative gaming and teamwork, and gaming characteristics and cybersecurity performance. Correlation must not be interpreted as proof of causation.

Independent-samples t-tests may compare relevant groups. Paired-samples t-tests may compare pre-test and post-test scores. ANOVA may compare multiple groups based on game genre or gaming profile. Regression analysis may examine whether gaming variables predict cybersecurity performance after considering prior computer science knowledge, cybersecurity exposure, programming experience, and academic background.

Qualitative interview and observation data may be analyzed thematically. Possible themes include learning through failure, strategic thinking, pattern recognition, teamwork, confidence, motivation, competition, distraction, excessive use, and transfer of skills.

18. Real-Life Educational Applications and Case Examples

Phishing as a Detective Challenge: Students examine fictional messages and identify suspicious sender information, misleading links, urgent language, unexpected attachments, and requests for credentials. Students must explain their reasoning rather than merely guess.

Incident Response Simulation: Teams receive fictional evidence such as repeated failed logins, unusual login timing, suspicious email, unexpected file activity, and abnormal account behavior. They must decide what evidence is most important, what additional information is needed, and what actions should be prioritized.

Strategy and Risk Prioritization: Students receive a fictional organization with limited resources and must prioritize security awareness, multi-factor authentication, updates, backups, monitoring, or other defensive controls. They justify decisions using risk-based reasoning.

Puzzle-Based Digital Forensics: Students receive fictional clues and reconstruct the most likely sequence of events. This supports chronology, evidence evaluation, pattern recognition, and reasoning under uncertainty.

Cooperative Cybersecurity Mission: Students take complementary roles, such as evidence reviewer, incident analyst, response planner, and documentation officer. The exercise demonstrates the importance of information sharing and coordinated decision-making.

19. Potential Findings and Interpretation

Students who frequently play strategy or puzzle games may perform better on selected reasoning tasks. Such results could suggest a relationship between game demands and transferable abilities, although self-selection must be considered because analytically inclined students may prefer challenging games.

Total gaming hours may show little or no direct relationship with cybersecurity performance. This would support the argument that what students play and how they engage may matter more than duration alone.

The intervention may increase engagement and participation. If the experimental group also improves more than the comparison group on objective knowledge and practical assessments, stronger evidence would exist for the educational value of structured game-based cybersecurity learning.

Some students may report that uncontrolled gaming interferes with studies, sleep, or time management. Such findings would reinforce the importance of balance and responsible use.

20. Discussion

The expected contribution of this study is to replace simplistic arguments about gaming with a more precise model. The important questions are which games, which skills, how much engagement, under what conditions, how skills are transferred, and how outcomes are measured.

Gaming should not be considered a substitute for cybersecurity education. Instead, it may act as a skills-development environment.

The strongest model is:
Existing Interest → Transferable Ability → Structured Education → Practice → Feedback → Measurable Competence.

For example, puzzle-solving may support pattern recognition, which can then be connected with log-analysis instruction and practical exercises. Strategic gaming may support consequence analysis, which can be connected with risk assessment. Cooperative gaming may support communication experiences that can be deliberately translated into incident-response teamwork. Repeated failure may support persistence that can be used in debugging and technical investigation.

This framework explains why ordinary gaming may sometimes support learning but cannot independently create cybersecurity competence.

21. Educational Implications

Schools should use existing student interests responsibly. Challenges, levels, feedback, missions, and progression can support motivation when aligned with clear learning objectives.

Every game-based activity should answer: What should students know or be able to do after this activity?

Reflection is essential. After completing an activity, students should discuss what happened, what evidence they used, what strategy worked, what failed, why it failed, which cybersecurity principle was involved, and how the lesson applies to defensive practice.

Competition must be managed carefully. It can motivate some students but discourage others. Educational design should balance competition with collaboration, individual progress, constructive feedback, and inclusive participation.

Ethical education must remain central. Students should understand authorization, privacy, legality, responsible disclosure, and professional responsibility. Activities should never encourage unauthorized access to real systems.

22. Limitations of the Proposed Study

Gaming behavior may be self-reported and therefore subject to inaccurate estimates. Students' game preferences may change over time. Causation is difficult to establish from observational relationships. A limited sample may reduce generalizability. Novelty effects may influence the intervention. Teacher effectiveness can affect learning

outcomes. Not every useful skill developed through gaming can be measured easily, and short-term assessment cannot establish long-term professional cybersecurity competence.

23. Ethical Considerations

Participation must be voluntary. Required parental or guardian consent must be obtained. Student privacy must be protected and identifying information should be anonymized. Participants must be free to withdraw. The research must not encourage excessive gaming. Cybersecurity activities must be legal and authorized. No participant should be instructed to access real systems without permission. Practical activities should use simulations, isolated laboratories, or intentionally designed educational environments. The research should not reward unhealthy amounts of gaming, and potential negative effects related to competition or stress should be considered.

24. Recommendations

1. Move beyond total screen time and distinguish gaming duration from game type, complexity, and purpose.
2. Integrate purposeful cybersecurity challenges such as scenario-based puzzles, phishing analysis, incident-response simulations, team missions, and authorized CTF activities.
3. Measure actual competence through knowledge and practical assessments rather than enjoyment alone.
4. Connect gaming skills explicitly with cybersecurity concepts.
5. Encourage balance so gaming does not interfere with education, sleep, health, relationships, or responsibilities.
6. Use a mixed instructional model combining explanation, reading, demonstration, practical activity, game-based challenge, reflection, and assessment.
7. Train teachers in selecting tools, designing activities, managing competition, evaluating learning, and maintaining ethical boundaries.
8. Conduct longitudinal studies to investigate long-term outcomes.

25. Suggestions for Future Research

Future researchers may investigate differences between individual game genres, long-term cybersecurity skill retention, inclusive game-based cybersecurity education, cross-cultural comparisons, relationships between gaming and programming skills, virtual and augmented reality cybersecurity simulations, AI-based adaptive cybersecurity games, the role of motivation, differences between entertainment games and serious games, and relationships between gaming, creativity, and defensive security problem-solving.

26. Conclusion

Cybersecurity education requires more than memorization. Students must learn to analyze, investigate, reason, communicate, adapt, and solve problems responsibly. The popularity of video games among young people raises an important educational possibility: some gaming experiences may provide repeated practice in abilities that can support later cybersecurity learning.

This paper adopts a balanced position. Gaming does not automatically transform students into cybersecurity experts. Cybersecurity competence requires specialized knowledge, practical experience, ethical judgment, and measurable skills. At the same time, it would be inaccurate to assume that all gaming is educationally meaningless.

Games can require problem-solving, pattern recognition, strategic planning, persistence, adaptation, decision-making, communication, and collaboration. These abilities may become educationally valuable when deliberately connected with formal cybersecurity instruction.

The most defensible conclusion is that gaming may provide a foundation for selected transferable abilities, but those abilities require deliberate educational translation before they become meaningful cybersecurity competencies.

The proposed mixed-method research design offers a practical way to test these relationships scientifically through gaming profiles, objective assessments, practical cybersecurity tasks, comparison groups, pre-test/post-test measurement, observation, and interviews.

The strongest educational approach is not to replace teachers with games or replace cybersecurity instruction with entertainment. Traditional teaching can provide theoretical foundations. Practical laboratories can develop technical competence. Game-based challenges can increase active participation. Simulations can provide safe practice. Reflection can transform experience into understanding. Assessment can determine whether genuine learning has occurred.

In conclusion, balanced and purposeful video-game engagement has the potential to support selected foundational skills relevant to cybersecurity learning among high school computer science students. Its greatest educational value is likely to emerge when gaming experiences are carefully connected with measurable learning objectives, practical cybersecurity activities, responsible use, ethical principles, and structured reflection. Gaming should therefore be understood not as a shortcut to cybersecurity expertise, but as one possible bridge through which students can develop curiosity, persistence, analytical habits, and problem-solving abilities that support their journey toward future cybersecurity competence.

Declaration by Author:

Ethical Approval: ***Approved***

Acknowledgement: "*To My Parent and Teachers, they guide me and support me to bring towards success, also to the people of my country."*

Source of funding: *None*

Conflict: *Author have no conflict of interest.*

References

Amjad, M. (2025). Unlocking cybersecurity: A game-changing framework for training and awareness—A systematic review. Human Behavior and Emerging Technologies.

Giannakoulas, A., & Xinogalos, S. (2024). Studying the effects of educational games on cultivating computational thinking skills among primary school students: A systematic literature review. Journal of Computers in Education, 11, 1283–1325.

Ng, C. Y., & Hasan, M. K. B. (2025). Cybersecurity serious games development: A systematic review. Computers & Security, 150, 104307.

National Institute of Standards and Technology. (2020). Workforce Framework for Cybersecurity (NICE Framework), NIST Special Publication 800-181 Revision 1.

National Institute of Standards and Technology. (2025). NICE Framework: Current Versions.

National Institute of Standards and Technology. (n.d.). NICE Framework K12 Frequently Asked Questions.

Weeratunge, N. H., Hjelsvold, R., & Katt, B. (2026). A systematic scoping review on game-based cybersecurity awareness education. International Journal of Information Security.

The association between video game play and cognitive ability: A systematic review and meta-analysis. (2026). Acta Psychologica, 107110.

Using serious games and digital games to improve students' computational thinking and programming skills in K-12 education: A systematic literature review. (2025). Technologies, 13(3), 113.

Gamification in cybersecurity education: A state of the art review and research agenda. (2024). Journal of Applied Research in Higher Education, 17(4), 1162–1180.

From CTF to competence: UX-driven and didactic foundations for gamified cybersecurity training platforms. (2026). Applied Sciences.

Damenu, T. K., Gökbay, İ. Z., Covaci, A., & Li, S. (2025). Cyber security educational games for children: A systematic literature review.

Gullali Niazai Completed ***BS (Computer Science)*** degree, now working as ***an independent researcher***, her area of interest is ***Computer Science and Cybersecurity.***