CYBERBEANGAMES: THE GAMIFICATION OF CYBERSECURITY EDUCATION

Lynda Levy Faculty Mentor: Weihao Qu Faculty Mentor: Brian Callahan

Monmouth University Department of Computer Science and Software Engineering

Research Introduction

As digital threats continue to evolve, engagement in cybersecurity education has seen a marked decline — traditional methods such as lengthy instructional videos followed by perfunctory quizzes have proven insufficient in fostering meaningful awareness of online safety. This research addresses that gap by offering a framework for more effective cybersecurity education, with particular focus on internet safety and phishing scam prevention, applicable to both academic and professional settings.

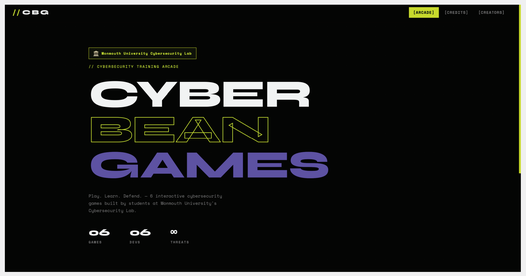

Figure 1. Login Screen for CyberBeanGames.

Utilizing CyberBeanGames.com, a website created by students and professors at Monmouth University, we can empower students to design and develop educational games. This approach serves a dual purpose: reinforcing the creators' own understanding of the subject matter while simultaneously providing an engaging and accessible learning experience for all participants.

CyberBeanGames Platform

The CyberBeanGames platform currently features six (6) educational games covering topics such as phishing scam detection, access control, password security, and malware awareness. Before and after each game, users are questioned about their knowledge of various cybersecurity concepts and the results indicate that participants answered significantly more questions correctly after completing the games, demonstrating a measurable improvement in awareness of cybersecurity and knowledge retention.

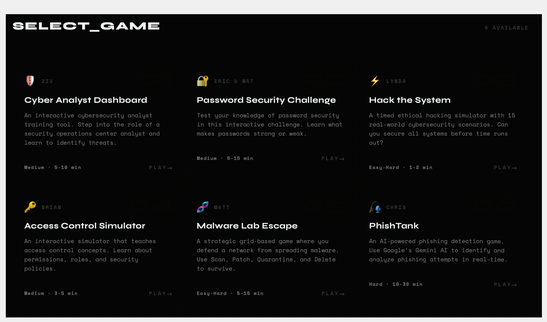

Figure 2. Game Selection Screen for CyberBeanGames.

Statistics and Cybersecurity Education

Out of 5,000 K-12 organizations between July 2023 and ecember 2024...

- 82% of reporting K-12 schools experienced cyber threat impacts [1]
- 14,000 security events during the reporting period [1]
- 9,300 confirmed cybersecurity incidents in that same timeframe [1]

espite the growing prevalence of cyber threats, cybersecurity education remains largely ineffective — traditional awareness training such as compliance videos and static slideshows fails to engage learners, resulting in poor retention of critical security practices [2]. Research [3] has shown that users remain highly susceptible to phishing attacks even after completing standard training, underscoring NIST's position that effective cybersecurity education must be continuous, interactive, and contextually relevant rather than a one-time event [4].

Interviews and Testimonials

Interviews with Professor u and student game creators revealed consistent support for the effectiveness of game-based cybersecurity education. Professor u noted that in a Spring 2025 test, 9 out of 10 students fell for a phishing scam, underscoring the inadequacy of traditional training methods. His experience running a summer camp with 20 students confirmed that small, browser-based games that could be completed in under five minutes were highly effective at teaching individual concepts. Student creators echoed these findings — Matt, who had no prior cybersecurity background, reported learning significantly more than just the basics while building his game. Ziv similarly observed that players came away with a stronger understanding of how to identify phishing attempts and protect their passwords. Both students agreed that peer-made games work best alongside formal education, offering an interactive and accessible complement to traditional classroom instruction.

Research Results

ata was collected from 11 participants between ebruary and March 2026. Key findings include:

- **100% of participants** gave the platform a rating of 5 out of 5
- **Post-game quiz scores** were consistently higher than pre-game scores among all participants who completed a game
- **5 out of 6** participants who completed a post-game quiz scored perfectly
- **9 out of 11** participants came from CS/IT backgrounds, suggesting strong interest from technically-minded users
- Participants with **no prior training** still performed well post-game, suggesting the games are effective regardless of background
- The platform was accessed across **Mac, Windows, and iPhone**, demonstrating cross-device accessibility
- **4 game creators** reported that building the games reinforced their own cybersecurity knowledge
- All 4 creators said they would **recommend this as a class assignment**

Conclusion and Future Research

Conclusion: Traditional cybersecurity education methods have proven insufficient in producing lasting awareness among students and professionals. CyberBeanGames.com, developed by students and faculty at Monmouth University, offers a more engaging alternative. With all participants rating the platform 5 out of 5 and post-game scores consistently outperforming pre-game scores, the findings confirm that game-based learning drives stronger knowledge retention while empowering student creators in the process.

uture irections: This investigation lays the groundwork for further research in cybersecurity education:

- **Expanded User/Creator Studies:** uture research should include larger and more diverse participant groups across different academic and professional settings to validate the effectiveness of game-based cybersecurity education at scale. Additionally, having more students create games will ensure that there is a game for every type of participant.
- **Pre/Post Assessment Integration:** Incorporating structured pre and post assessments into the CyberBeanGames platform will allow for more rigorous measurement of learning outcomes and behavioral change.
- **Curriculum Integration:** urther work should explore how platforms like CyberBeanGames can be formally embedded into existing cybersecurity curricula at the high school and university level.

Figure 3. QR code for CyberbeanGames.com

References

[1] CIS, "CIS MS-ISAC K-12 Cybersecurity Report," https://www.cisecurity.org/insights/white-papers/2025-k12-cybersecurity-report, 2025, [Online; accessed 18-Mar-2026].

[2] C. Hadnagy and M. Fincher, *Phishing ark Waters*. Wiley, 2015.

[3] P. Kumaraguru, Y. Rhee, A. Acquisti, L. Cranor, J. Hong, and E. Nunge, "Protecting people from phishing: the design and evaluation of an embedded training email system," in *Proceedings of the SIGCHI Conference on Human actors in Computing Systems*, 2007.

[4] National Institute of Standards and Technology, "Building an information technology security awareness and training program," NIST, Tech. Rep. SP 800-50, 2003.