NATIONAL ENGITECH DIGEST

VOL. 1 ISSUE 1

e-ISSN: 3030-5969

Gaming Cyber Awareness Among ICT Students in Ungku Omar Polytechnic

Azrahayu Abdul Aziz [1], Afifah Nailah Muhamad [2]
Information Technology & Communication, Ungku Omar Polytechnic, Jalan Raja Musa Mahadi, 31400 Ipoh
[1]aazrahayu@puo.edu.my, [2]anailah@puo.edu.my

Abstract:

In today's digital age, online gaming has become a significant aspect of youth culture, with millions of young players engaging in virtual worlds daily. However, the rise in online gaming's popularity has also brought an increase in cyber threats, making it essential to educate young gamers about cybersecurity. Gaming cyber awareness for education aims to bridge the gap between the fun of gaming and the importance of cybersecurity knowledge. By integrating cybersecurity education into gaming, we can equip young players with the skills and awareness needed to navigate online environments safely and responsibly. This study addresses the shortcomings of traditional cybersecurity education methods by introducing an innovative approach through the "Visual Game for Cybersecurity Education by using Roblox Studio application." The conventional methods, relying on passive learning, struggle to engage the current generation actively. The lack of awareness about cybersecurity risks necessitates a dynamic solution. The research aims to design a gaming method that not only supports effective education but also offers an immersive learning experience. Using Agile Methodology, the iterative development approach allows early player engagement, fostering continuous improvement. The functional requirements, such as puzzles about cybersecurity and exposure to cyber threats, ensure active learning and awareness. Non-functional aspects, including performance, reliability, and security, guarantee a seamless and secure gaming experience. The outcome of this approach lies in providing an engaging learning environment and real-world simulations, enhancing problem-solving skills. Improvement suggestions include addressing technical requirements and optimizing resource-intensive aspects. The study concludes that balancing accessibility, technical considerations, and the learning curve is crucial for maximizing the project's educational impact.

Keywords: Cybersecurity Education, Gamified Learning, Agile Methodology, Interactive Learning.

Introduction

In the landscape of contemporary education, traditional methods employed for cybersecurity education often fall short of capturing the attention and interest of today's generation (Nelson, C.D, 2024). These conventional approaches, predominantly reliant on passive learning mechanisms like lectures and textual materials, face a significant challenge in engaging students actively. The evolving nature of cyber threats demands a paradigm shift in educational strategies to ensure that learners not only acquire essential cybersecurity knowledge but do so in an immersive and engaging manner.

Compounding the challenge is the pervasive lack of awareness and understanding of cybersecurity risks and best practices among the general public. This deficiency underscores the need for innovative educational interventions. The "Visual Game for Cybersecurity Education" project responds to these issues by addressing the limitations of conventional education and aiming to foster a proactive and engaging approach to cybersecurity learning (Sharma, R & Thapa S, 2023). The primary objectives of this project are twofold. First, we aim to design a gaming method that enhances the effectiveness of cybersecurity education, offering a more supportive learning environment for users. Second, the project seeks to develop an interactive game that immerses players in a dynamic learning experience, allowing them to grasp cybersecurity concepts and best practices through the resolution of puzzles and challenges.

The game's system scope entails creating a virtual scenario where players navigate through a room filled with clues and challenges, providing a practical and engaging platform for cybersecurity education. Designed for users who aspire to understand cybersecurity concepts while enjoying the process of solving puzzles and challenges, the project targets high school students. The aim is to equip users with essential skills to safeguard themselves from cyber threats, aligning with the specific needs of this demographic.

Research Methodology

The research methodology for developing the gaming cyber awareness application involves a systematic approach to ensure a comprehensive and effective solution. The process is divided into several key phases, each with specific objectives and deliverables. This methodology will outline the steps taken to design, develop, and implement the application. The development of the gaming cyber awareness application involves identifying key requirements through surveys, literature reviews, and community feedback; creating a detailed design with user personas, wireframes, and core functionalities; outlining technical specifications and planning with appropriate technologies, architecture, and timelines; building the application with frontend and backend development, ensuring smooth integration; conducting comprehensive testing and quality assurance; deploying and launching the app with monitoring and promotion; and providing ongoing support and maintenance through user feedback, regular updates, and community engagement.

Analysis and Discussion

In establishing the requisites for the project, a distinction is drawn between functional and non-functional components to ensure a comprehensive framework for the gaming experience (Kumar, D et al., 2022). Functionally, the project aims to cultivate an engaging and educational gameplay atmosphere. The game will integrate cybersecurity-related puzzles, enabling players to actively learn and respond to diverse cyber threats. Players will also have the opportunity to explore solutions on the internet, fostering a dynamic and interactive learning process. Additionally, the game will expose players to cyber threats, especially those encountered during internet browsing, equipping them with the knowledge to evade falling victim to such threats (Tinubu,C.O at al., 2023) .

On the non-functional aspect, the project encompasses various dimensions to ensure a robust and user-friendly gaming experience. Performance is optimized to support up to 10 users per server across five servers, with loading screens facilitating a swift start. Reliability is prioritized to minimize crashes, freezes, or technical disruptions that could compromise player experience. Availability is a key focus, allowing users to access and play the game at their convenience. In terms of maintainability, the system is designed with modularity in mind, facilitating easy updates, bug fixes, and future enhancements. Regular backups of game data and server configurations ensure recoverability in case of data loss.

The game's capacity accommodates more than 10 players simultaneously, and serviceability is maintained through prompt issue identification and resolution. Security is paramount, incorporating anti-cheat measures to protect user data and prevent unauthorized access (Ibrahim, A, 2024). Manageability involves regular oversight of game services for ongoing improvement. The environmental aspect is designed to create an easy-to-learn in-game environment, fostering user engagement. Data integrity is ensured through safeguards against corruption or tampering, and interoperability allows users to play the game on various platforms, including PC and mobile devices. Usability is enhanced with clear instructions, helpful hints, and appropriate feedback guiding players through educational challenges.

Concerning hardware and software requirements, developers need a laptop with specific specifications, while users require a mobile device meeting certain criterion (Sun, AN et al., 2022). Software requirements include Roblox Studio for developers and the Roblox application for users, each with recommended versions.

The system configuration for accessing the game involves downloading Roblox, creating an account, and installing the app. Users can then search for the game, "We Are Not Safe!" and initiate gameplay by following on-screen instructions to achieve set goals.

Addressing security requirements, the project prioritizes confidentiality by storing user data on the secure Roblox server, accessible only by authorized users (Abilkaiyrkyzy, A. et al., 2023). Integrity is maintained through monitoring player behavior and promptly addressing cheating or hacking attempts. Availability is ensured by providing contact information for players to report bugs, and accountability is demonstrated by swiftly fixing reported issues.

In response to the outlined project requirements, our team delved into the design phase, crafting interfaces that embody the principles of functionality, reliability, and user accessibility. The interfaces, exemplified by Figures 1 and 2, are pivotal elements in bringing our educational gaming vision to fruition. These interfaces serve as tangible manifestations of our commitment to creating a user-centric and educationally enriching gaming experience. They play a crucial role in enhancing the user experience by providing an intuitive main menu (Figure 1) and customizable settings (Figure 2) on smartphones.

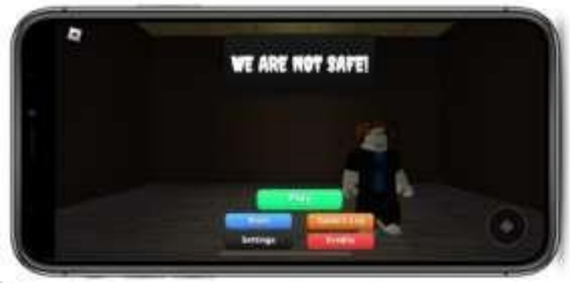

Figure 1. Main menu in Smartphone

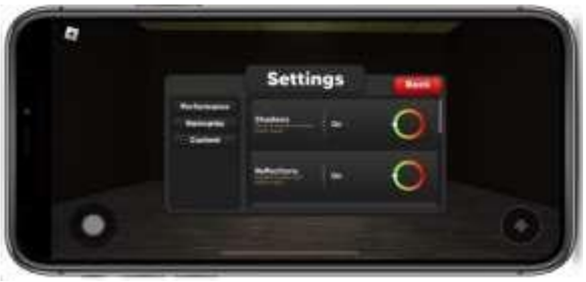

Figure 2. Setting in Smartphone

Conclusion and Recommendation

In conclusion, the development and implementation of the cyber education escape game represent a significant leap forward in cybersecurity education. The project's unique advantage lies in offering users a distinctive and engaging learning experience. By adopting a game format, the project transforms cybersecurity education into a fun and interactive endeavor, fostering active participation and enhancing knowledge retention (Zhao, T et al., 2024). The incorporation of real-world simulations within the game provides players with authentic cybersecurity challenges, thereby improving problem-solving and critical thinking skills.

In terms of advantages, the project's engaging learning experience is paramount. By leveraging the game format, users are drawn into an educational environment that is not only informative but also enjoyable. This approach encourages active participation and ensures that users remain invested in the learning process. Additionally, the use of real-world simulations elevates the project's educational value. By presenting users with authentic cybersecurity challenges and scenarios, the game goes beyond theoretical concepts. This practical application enhances problem-solving and critical thinking skills, preparing users for real-world situations in the realm of cybersecurity.

On the flip side, the project comes with its share of challenges. A notable drawback lies in its technical requirements. The game's reliance on specific hardware and software configurations, such as graphics capabilities and the use of Roblox, may limit accessibility. Some users might face challenges downloading Roblox based on memory and storage constraints, potentially hindering their participation. Furthermore, the creation and maintenance of a complex online game introduce resource-intensive demands. The project necessitates dedicated servers, frequent upgrades, and ongoing technical support. These requirements contribute to the time-consuming, expensive, and labor-intensive nature of maintaining such a sophisticated educational platform.

Another challenge lies in the learning curve. Depending on the complexity of the game, users may encounter a learning curve as they familiarize themselves with the mechanics and concepts presented. This learning curve could impact the initial user experience, requiring additional time and effort for users to grasp the intricacies of the game.

In essence, while the cyber education escape game brings innovation to cybersecurity education, its effectiveness is accompanied by certain challenges. Striking a balance between accessibility, technical requirements, and the learning curve will be crucial for optimizing the educational impact of the project.

References (Use APA format)

Haleem, A., Javaid, M., Qadri, M. A., & Suman, R. (2022). Understanding the role of digital technologies in education: A review. *Sustainable Operations and Computers*, *3*, 275-285.

Criollo-C, S., Abad-Vásquez, D., Martic-Nieto, M., Velásquez-G, F. A., Pérez-Medina, J. L., & Luján-Mora, S. (2021). Towards a new learning experience through a mobile application with augmented reality in engineering education. *Applied Sciences*, *11*(11), 4921.

Nelson, C. D. (2024). *Hacking the learning curve: Effective cybersecurity education at scale*. Arizona State University.

Sharma, R., & Thapa, S. (2023). Cybersecurity awareness, education, and behavioral change: strategies for promoting secure online practices among end users. *Eigenpub Review of Science and Technology*, *7*(1), 224-238.

Behutiye, W., Karhapää, P., López, L., Burgués, X., Martínez-Fernández, S., Vollmer, A. M., ... & Oivo, M. (2020). Management of quality requirements in agile and rapid software development: A systematic mapping study. *Information and software technology*, *123*, 106225.

Kumar, D., Kumar, A., & Singh, L. (2022). Non-functional requirements elicitation in agile base models. *Webology*, *19*(1), 1992-2018.

Tinubu, C. O., Falana, O. J., Oluwumi, E. O., Sodiya, A. S., & Rufai, S. A. (2023). PHISHGEM: a mobile game-based learning for phishing awareness. *Journal of Cyber Security Technology*, *7*(3), 134-153.

Ibrahim, A. (2024, February). Guarding the Future of Gaming: The Imperative of Cybersecurity. In *2024 2nd International Conference on Cyber Resilience (ICCR)* (pp. 1-9). IEEE.

Sun, N., Li, C. T., Chan, H., Le, B. D., Islam, M. Z., Zhang, L. Y., ... & Armstrong, W. (2022). Defining security requirements with the common criteria: Applications, adoptions, and challenges. *IEEE Access*, *10*, 44756-44777.

Abilkaiyrkyzy, A., Elhagry, A., Laamarti, F., & Elsaddik, A. (2023). Metaverse key requirements and platforms survey. *IEEE Access*.

Zhao, T., Gasiba, T., Lechner, U., & Pinto-Albuquerque, M. (2024). Thriving in the era of hybrid work: Raising cybersecurity awareness using serious games in industry trainings. *Journal of Systems and Software*, *210*, 111946.

nd Software, 210, 111946.