

A Rapid Review on Serious Games for Cybersecurity Education: Are “Serious” and Gaming Aspects Well Balanced?

Miriana Calvano¹, Federica Caruso², Antonio Curci¹, Antonio Piccinno¹ and Veronica Rossano¹

¹University of Bari Aldo Moro, Via Orabona 4, 70125, Bari, Italy

²University of L'Aquila, Via Vetoio, 67100, L'Aquila, Italy

Abstract

As technology becomes increasingly integrated into our daily lives, cybersecurity has become a necessity that demands attention. In fact, possessing a basic understanding of cybersecurity techniques, concepts, and tools is essential for individuals to remain safe and secure. Serious Games are gaining popularity as educational tools in cybersecurity due to their incorporation of engaging and motivating elements not typically present in traditional education, making the learning experience more engaging and motivating. However, the effectiveness of Serious Games in promoting learning is heavily contingent on their design, particularly the balance achieved between the serious educational content and the engaging gaming elements. This paper aims to analyze 15 serious games for cybersecurity, evaluating the balance between their educational and gaming aspects. By identifying the key factors that influence the design and effectiveness of serious games for cybersecurity education, this paper provides valuable insights for educators, managers, and game designers interested in developing effective serious games in this domain.

Keywords

Serious Games, Cybersecurity, Education, Engagement

1. Introduction

Serious games are games that do not prioritize entertainment, enjoyment, or fun as their primary purpose [1]. They can be used for various applications with different goals, offering a new way to experience education [2]. By incorporating gaming aspects, serious games can support the learning process and make it more engaging for all parties involved; this can increase the amount of information learners acquire by associating it with a positive experience and eliminating boredom and frustration [2, 3, 4]. Cybersecurity education is one area where serious games are increasingly widely used today [5, 6]. In fact, as technology increasingly impacts people's lives, its innovative services and commodities have downsides, such as security attacks and privacy violations [7, 8]. Educating individuals about cybersecurity issues is crucial to promote awareness, but unskilled or uninterested individuals may find the training process


IS-EUD 2023: 9th International Symposium on End-User Development, 6-8 June 2023, Cagliari, Italy

✉ miriana.calvano@uniba.it (M. Calvano); federica.caruso1@univaq.it (F. Caruso); antonio.curci@uniba.it (A. Curci); antonio.piccinno@uniba.it (A. Piccinno); veronica.rossano@uniba.it (V. Rossano)

🆔 0000-0002-9507-9940 (M. Calvano); 0000-0002-6167-3896 (F. Caruso); 0000-0001-6863-872X (A. Curci); 0000-0003-1561-7073 (A. Piccinno); 0000-0002-4079-9641 (V. Rossano)



© 2023 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

difficult or uninteresting [9, 10]. Thus, serious games can be helpful by integrating fun, playful, and pleasurable aspects into the learning process [6]. This research aims to examine 15 serious games for cybersecurity education by conducting a rapid review of their main aspects. The motivation behind choosing serious games instead of capture the flag (CTF) lies in the fact that the latter only focuses on the assessment of cybersecurity knowledge and skills, while serious games aim at broader learning objectives by increasing people's awareness in the field. More specifically, serious games do not only convey competences, but support the learning process as a whole. The serious games were chosen based on their free online availability and frequent mention in multiple online resources on this topic. The objective is to determine whether these serious games present a balanced combination of educational and gaming aspects by qualitatively analyzing their main characteristics. Specifically, concerning the educational aspects, the learning objectives and the strategies employed to address them were [11]. At the same time, the User Interface (UI) elements and mechanics were analyzed for the gaming elements. It is crucial for serious games to equally integrate both aspects to achieve their intended learning and entertainment purpose [2, 3, 4, 12]. A poor user experience, lack of gaming elements, or cumbersome mechanics can negatively affect players' engagement and flow state [2, 3, 4]. The results of this rapid review will provide valuable insights into the current state-of-the-art in this field. They may stimulate future discussions on how to design serious games for cybersecurity in a balanced and effective way.

2. Rapid review

This section briefly analyzes the 15 serious games, indicating their main characteristics and the balance between gaming and educational aspects.

Keep Tradition Secure¹ is a quiz-based game designed to test users' knowledge of both cybersecurity and Texas A&M University traditions, such as a secure way to use public wireless networks and most known places in the campus. The game targets general users and can be played online on desktop and mobile devices and in a location-based mode using a mobile device. Upon analyzing this serious game, it is evident that it lacks audio and sensory elements, and the User Interface (UI) is not visually appealing except for the use of real-life pictures of places and objects. The game's primary objective is to impart knowledge rather than provide an engaging game-based learning experience. The absence of win/loss conditions or punishment/reward mechanisms highlights this.

Targeted Attack: The Game² is a quiz-based serious game that explores the topic of targeted attacks, as the title suggests. The serious game can be played on mobile or desktop devices. Within the game, the player follows the storyline and takes actions as a security team member for an organization launching a mobile payments app with biometric authentication. The serious game consists of a series of multiple-choice questions that lead to different changes in the storyline, allowing the player to make decisions about cybersecurity matters. The serious game has a futuristic design that provides context and emphasizes the seriousness of the situation. Videos are included at each step to give the user a full understanding of the situation and are

¹<https://keeptraditionsecure.tamu.edu/>

²<http://targetedattacks.trendmicro.com/cyoa/en/>

essential to play the serious game. Transitions are added between each video to provide a smooth and pleasant experience. Upon analyzing this serious game, experienced gamers may find the lack of rich elements like avatars, virtual game worlds, and game mechanics boring. Therefore, it is evident that this serious game focuses heavily on educational aspects rather than gaming aspects.

Data Center Attack: The Game³ covers the topic of data center attacks and has the same mechanics, UI elements, and rules as *Targeted Attack: The Game*. The player must protect a hospital from data center attacks by making the right decisions regarding security measures and recovery techniques. The same considerations as the previously mentioned game apply.

Cybersecurity Lab⁴ is a game that aims to teach young people aged 10 to 17 years old how to act and think when facing various cyber attacks (e.g., password cracking, social engineering, and network security) to defend an organization that provides social media platform services. This serious game can be played on any device with an internet connection, modern browser, and keyboard. Players learn concepts and acquire skills by solving exercises and completing challenges. The serious game cannot be completed unless all tasks are carried out successfully, emphasizing its serious aspect. Completing challenges with a high level of accuracy earns the player more money, which can then be used to purchase more expensive tools to defend the organization. Cybersecurity is the core theme of the serious game, reflected in its dark theme, which may encourage players to take the game seriously and learn about real-world issues. However, upon analyzing this serious game, it appears that it may feel too static and not motivate players to finish it due to a large number of challenges and exercises required to reach the end. This could result in frustration and negatively impact the player's flow state, despite the balance between educational and gaming purposes.

Hot Spot Hunt for the Violations!⁵ is a serious game designed to teach players how to recognize elements that can cause cyber-attacks, such as leaving a password on a desk or personal information unattended. The serious game targets not a specific kind of user, and it can be played on desktop and mobile devices. The serious game takes place in a fictional office with various artifacts and graphical elements but lacks audio and sensory elements. Upon analyzing this serious game, it appears that it focuses more on knowledge acquisition than gaming aspects, as no punishment or reward mechanisms have been integrated. However, to emphasize the importance of raising awareness about the potential reasons for being a victim of a cyber-attack, win/lose conditions have been integrated into the gameplay. In fact, the serious game can only be completed successfully if the player identifies all the "threatening" elements. Therefore, the game and learning aspects appear not well-balanced.

The missing link⁶ is a serious game aiming at assessing cybersecurity knowledge and teaching useful tips for staying safe online. The serious game targets no specific kind of users, but university students and employees have access to additional features. The serious game can be played online using a laptop, desktop, or mobile device. The serious game consists of challenges to find the attacker, and even if the player selects the wrong answer, they can proceed to the next level. The serious game is set in an office, representing typical Western cultural

³<http://datacenterattacks.trendmicro.com/>

⁴<https://www.pbs.org/wgbh/nova/labs/lab/cyber/>

⁵<https://hotspot.livingsecurity.com/>

⁶<https://it.tamu.edu/missinglink/>

aspects and features, accurately mirroring the real-world scenario. The game lacks audio and sensory elements but is rich in visual elements, such as artifacts and character portraits, which increase players' interest. In addition, the presence of a storyline creates a mystery to enhance players' motivation and engagement. The game mechanics do not include a punishment/reward mechanism, but win/lose conditions are defined. Upon analyzing this serious game, it appears that it prioritizes gaming elements over serious purposes, resulting in an imbalance between game and learning aspects.

Permission Impossible: Teaching Firewall Configuration in a Game Environment⁷ is a serious game that focuses on technical cybersecurity issues, such as firewall configurations, network structures, and network security. The game can be played through a browser on any desktop or mobile device and targets a wide audience, including children, students, and adults [13]. The game has simple rules: it consists of 10 levels, each increasing in difficulty and introducing new concepts in network security. The player can choose any level to play from the beginning. Each level contains challenges in which firewalls must be constructed. The challenges in each level cannot be skipped but must be completed successfully to progress to the next level. The game immediately notifies the player when they make a mistake and prompts them to fix it, helping them extract ethical values from it. However, upon analyzing this serious game, the design seems outdated and unintuitive, which can negatively impact the player's ability to acquire knowledge. Therefore, this serious game seems to prioritize educational aspects over a smooth and engaging gaming experience.

Cyber Challenge⁸ is a quiz-based serious game that covers basic cybersecurity concepts to increase users' awareness and help prevent malicious activities. The serious game can be played on desktop and mobile devices. In detail, this serious game consists of protecting, defending, and striking a system by solving brain teasers and quizzes. The game focuses on punishment mechanisms and win/lose conditions: if a level is not passed successfully, the player must repeat it until they pass, emphasizing knowledge acquisition over player engagement. In addition, the serious lacks sensory elements and is poor in visual elements but employs audio elements at the start of each level. Therefore, upon analyzing this serious game, it appears that there is a major focus on acquiring knowledge rather than engaging players. Thus, the learning and gaming aspects appear not well balanced.

Aggie Life⁹ is a serious game that focuses on general cybersecurity knowledge and aims to provide tips on best practices in the field. Anyone can play the serious game, as it is web-based and playable from any device with a modern browser. In detail, this serious game is a board game in which movements are determined by a spinning wheel that indicates the number of blocks to move forward. In addition, the game appears easy to understand on the first try and has an intuitive and simple design. However, upon analyzing this serious game, it seems not strongly stimulate players' entertainment and engagement, except for the desire to reach the end with a high score. This suggests that the game's educational objective was primarily taken into account during design.

Google XSS Game¹⁰, is a serious game exploring the topic of Cross-Site Scripting (XSS)

⁷<https://groups.inf.ed.ac.uk/tulips/projects/1617/PermissionImpossible/>

⁸<https://www.cybermission.tech/#!/page/home>

⁹<https://it.tamu.edu/aggielife/question/1/>

¹⁰<https://xss-game.appspot.com/>

attacks. In detail, the player must complete challenges to progress to the next level, and cannot play the next level until the previous one is successfully completed. In addition, the player can toggle hints and suggestions to get help if they encounter problems. Upon analyzing this serious game, it appears that it presents a few game elements, lacking a virtual game world, storyline, and characters, which could negatively impact players' engagement. In addition, players with sufficient background knowledge of the topics presented may find the serious game intriguing and challenging, but the level of difficulty of each challenge is quite high and not suitable for those who are not familiar with the topic. Therefore, it is evident that the educational aspects of this serious game are more prominent than its gaming elements.

Cyber Awareness Challenge¹¹ is a quiz-based game that provides an overview of current cybersecurity threats and best practices for keeping information and information systems secure at home and work, for example how to avoid to be a victim of a phishing attack. This serious game is available on desktop and mobile devices. Being structured as a quiz game with questions to answer and brain teasers to solve, the serious game does not present any audio/sensory elements or a virtual game world, and it is characterized by a few visual elements such as a text panel and a progress bar. Nevertheless, even if there is a clear focus on "serious" purposes, popular game mechanics are not absent, such as punishment/reward mechanisms and win/lose conditions, to stimulate user engagement. In addition, each game level is introduced through TV news fragments to create a correspondence between the game and reality, which helps construct a story and increase attention. Therefore, upon analyzing this serious game, it is evident that it strikes a good balance between emphasizing cybersecurity concepts and incorporating game elements.

Cyber Threat Defender¹² is a card-based serious game that focuses on teaching cybersecurity strategies, assets, and attacks. The serious game requires a computer to download its launcher and targets middle- and high-schoolers aged 10 to 17 years old. Players take turns attacking or defending their opponent, earning or losing points depending on the correctness of their actions. The game emphasizes the concept of being "right" by successfully defending the organization and "wrong" otherwise, stimulating players' decision-making and problem-solving skills. The serious game's UI is composed of electrical circuits and pins in the background, reminding players of the domain they are operating in (cyber and network security). Upon analyzing this serious game, it appears that it is very simple in mechanics and does not present an involving storyline, but it can be very effective for those who enjoy card games, making it well-balanced in terms of educational and gaming elements.

The Weakest link, A User Security Game¹³ is a quiz-based serious game aiming at increasing awareness about cybersecurity risks and the appropriate behavior to adopt in suspicious circumstances. The game targets Information Technology (IT) professionals and can be played on desktop and mobile devices. The game is not rich in visual, audio, or sensory elements but is a quiz game in which each question corresponds to a workday, and the player's progress is indicated through a progress bar. Although the graphics are minimal, there is a visible emphasis on cybersecurity concepts, such as best practices for avoiding personal information theft. Game

¹¹<https://public.cyber.mil/training/cyber-awareness-challenge/>

¹²<https://cias.utsa.edu/ctd/play-online/>

¹³<https://www.isdecisions.com/user-security-awareness-game/>

mechanics, such as punishment/reward mechanisms and win/lose conditions, are integrated into the game. If the player selects the wrong answer, an explanation about the topic is provided, and the security score decreases, forcing the player to repeat the levels from the beginning. Thus, upon analyzing this serious game, it appears that it provides a well-balance between serious and game aspects.

Cybercity Chronicles¹⁴ is a mobile serious game that aims to sensitize people to the conscious use of the web and new technologies through a variety of characters and challenges. The game targets no specific kind of users and allows them to learn basic cybersecurity concepts by solving enigmas and reading hints provided by characters. Punishment/reward mechanisms and win/lose conditions are employed in the game to stimulate players' interest and attention. The game also features internal economies where players collect bitcoins to buy and upgrade equipment. Upon analyzing this serious game, it appears that it is rich in visual and audio elements, increasing player engagement and allowing them to enter a state of flow. The scenario is characterized by a wide range of characters, creating a dense and coherent storyline with different goals to reach. Therefore, this serious game can be considered an excellent example that perfectly balances gaming and learning aspects.

Google Interland¹⁵ is the most elaborate serious game analyzed in this study. It consists of four different and unrelated modules, each covering a topic related to how cybersecurity affects an individual's private life. These topics include how to protect personal devices, best practices for interacting with others online, preserving personal information while surfing the web, and learning how to distinguish between legitimate and false information. The serious game targets students aged 7 to 12 years old and can be played on any browser with mid to high technical specifications. In particular, the serious game consists of multiple challenges to complete, questions to answer, and riddles to solve. It is well-designed and rich in terms of UI elements, mechanics, and educational goals. Although the modules do not interfere with each other, the design elements follow the same theme in terms of the general look and feel. Differences can be found in colors, characters, and actions to perform. Therefore, upon analyzing this serious game, it appears that it provides a well-balance between serious and game aspects.

3. Discussion and conclusions

This paper reviewed 15 serious games related to cybersecurity, evaluating their design in terms of educational and gaming aspects to determine the balance between the two. The results showed that educational goals were prioritized over gaming elements in most cases (10 out of 15). This may be due to a lack of multidisciplinary involvement in serious game design, which can lead to a poor gaming experience and hinder knowledge acquisition. To address this imbalance, a balanced approach to cybersecurity-oriented serious game design is needed, along with the use of standardized and generalized methodologies that embody best practices. Game designers can create games that balance educational and gaming elements by considering the key factors identified in this review, resulting in an engaging and effective learning experience for players.

¹⁴<https://www.sicurezza.azionariale.gov.it/sisr.nsf/cybercity-chronicles.html>

¹⁵https://beinternetawesome.withgoogle.com/en_us/interland

This rapid review can be beneficial for those interested in selecting or developing serious games for cybersecurity education and training [14]. For example, educators and managers can use the findings to identify appropriate serious games for their students and employees to improve cybersecurity education and awareness. In conclusion, this paper provides valuable insights into serious games for cybersecurity education and highlights the need for a balanced approach to serious game design. Future research could expand on this work by analyzing a larger number of serious games to identify new results and limitations in the field, further enhancing the practical applications of this research.

Acknowledgments

This work was partially supported by project SERICS - "Security and Rights In the CyberSpace - SERICS" (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

References

- [1] V. S. Barletta, F. Caruso, T. Di Mascio, A. Piccinno, Serious games for autism based on immersive virtual reality: A lens on methodological and technological challenges, in: *International Conference in Methodologies and intelligent Systems for Technology Enhanced Learning*, Springer, 2023, pp. 181–195.
- [2] K. Mitgutsch, N. Alvarado, Purposeful by design? a serious game design assessment framework, in: *Proceedings of the International Conference on the foundations of digital games*, 2012, pp. 121–128.
- [3] B. Marne, J. Wisdom, B. Huynh-Kim-Bang, J.-M. Labat, The six facets of serious game design: a methodology enhanced by our design pattern library, in: *21st Century Learning for 21st Century Skills: 7th European Conference of Technology Enhanced Learning, EC-TEL 2012, Saarbrücken, Germany, September 18-21, 2012. Proceedings 7*, Springer, 2012, pp. 208–221.
- [4] L. A. Annetta, The "i's" have it: A framework for serious educational game design, *Review of general psychology* 14 (2010) 105–113.
- [5] M. Coenraad, A. Pellicone, D. J. Ketelhut, M. Cukier, J. Plane, D. Weintrop, Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games, *Simulation & Gaming* 51 (2020) 586–611.
- [6] S. Kulshrestha, S. Agrawal, D. Gaurav, M. Chaturvedi, S. Sharma, R. Bose, Development and validation of serious games for teaching cybersecurity, in: *Serious Games: Joint International Conference, JCSG 2021, Virtual Event, January 12–13, 2022, Proceedings 7*, Springer, 2021, pp. 247–262.
- [7] V. Kumar, M. A. Alqahtani, Cybersecurity awareness based on software and e-mail security with statistical analysis, *Computational Intelligence and Neuroscience* (2022). doi:<https://doi.org/10.1155/2022/6775980>.
- [8] M. T. Baldassarre, V. Santa Barletta, D. Caivano, D. Raguseo, M. Scalera, Teaching cyber security: The hack-space integrated model., in: *ITASEC*, 2019.

- [9] T. Alharbi, A. Tassaddiq, Assessment of cybersecurity awareness among students of majmaah university, *Big Data and Cognitive Computing* 5 (2021). URL: <https://www.mdpi.com/2504-2289/5/2/23>. doi:10.3390/bdcc5020023.
- [10] M. Khader, M. Karam, H. Fares, Cybersecurity awareness framework for academia, *Information* 12 (2021). URL: <https://www.mdpi.com/2078-2489/12/10/417>. doi:10.3390/info12100417.
- [11] V. S. Barletta, F. Cassano, A. Marengo, A. Pagano, J. Pange, A. Piccinno, Switching learning methods during the pandemic: A quasi-experimental study on a master course, *Applied Sciences* 12 (2022). URL: <https://www.mdpi.com/2076-3417/12/17/8438>. doi:10.3390/app12178438.
- [12] F. Caruso, T. Di Mascio, "designing ivr serious games for people with asd: An innovative approach", in: *Methodologies and Intelligent Systems for Technology Enhanced Learning, 10th International Conference. Workshops: Volume 2*, Springer, 2021, pp. 291–295.
- [13] S. Sehl, K. Vaniea, Permission impossible: Teaching firewall configuration in a game environment, in: *European Workshop on Usable Security, 2018*. URL: <https://eusec.cs.umd.edu/doi:https://dx.doi.org/10.14722/eurosec.2018.23006>, 3rd European Workshop on Usable Security, EuroUSEC 2018 ; Conference date: 23-04-2018.
- [14] F. Tommasi, C. Catalano, I. Taurino, Browser-in-the-middle (bitm) attack, *Int. J. Inf. Secur.* 21 (2022) 179–189. URL: <https://doi.org/10.1007/s10207-021-00548-5>. doi:10.1007/s10207-021-00548-5.