

Design of a Serious Game for Cybersecurity Education: Cyber Academy

Miriana Calvano¹, Antonio Curci^{1,2}, Antonio Piccinno¹ and Veronica Rossano¹

¹University of Bari "Aldo Moro", Department of Computer Science Via Edoardo Orabona, 4 70125 Bari, Italy

²University of Pisa, Department of Computer Science, Largo B. Pontecorvo, 3 56127, Pisa, Italy

Abstract

The exponential spread of technology and the increase of sophistication of internet services has brought countless advantages and has allowed huge steps towards scientific progress, but it also hides challenges, risks, and threats that individuals have to be aware of. Cybersecurity is the field of computer science that deals with threats that come from technology in all of its facets. This implies that final users have to be appropriately educated and trained in order to be able to protect themselves from all the risks that hide behind the use of daily technology. This work aims at proposing a serious game for cybersecurity education, which incorporates realistic scenarios and challenges concerning their knowledge of cybersecurity principles and techniques.

Keywords

Cybersecurity Education, Serious games, Game-based Learning, Gamification, Design,

1. Introduction

Technology and learning have always had a deep and interconnected relationship. Throughout human history, a lot of ways have been thought and implemented with the aim to enhance our ability to learn, understand, and communicate. Through the employment of technology the learning process is becoming more accessible, engaging, and personalized, tailoring educational experiences to individual needs and preferences [1]. In this regard, due to the growth of available data and, at the same time, to the increasing reliance of digital technology, new challenges and issues emerged [2]. In this context, cybersecurity has become crucial for individuals and organizations; it refers to "the process of protecting information by preventing, detecting, and responding to attacks" [3, 4]. To reduce the likelihood and impact of cyber-attacks it is necessary to teach individuals cybersecurity related concepts, threats, and possible ways to identify potential threats [5].

With the objective of engaging learners by providing an immersive and more effective learning experience, serious games are increasingly being used in a variety of fields (e.g., healthcare, education, business...) [6][7][8][9]. In fact, many studies demonstrate that the employment of game-based learning methodologies can positively impact the process of acquiring new


2nd International Workshop on CyberSecurity Education for Industry and Academia (CSE4IA 2024)

✉ miriana.calvano@uniba.it (M. Calvano); i.antonio.curci@uniba.it (A. Curci); antonio.piccinno@uniba.it (A. Piccinno); veronica.rossano@uniba.it (V. Rossano)

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



© 2024 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)

knowledge and gaining skills [10]. Defined by Kalamputzis, serious game are "games that do not have entertainment, enjoyment, or fun as their primary purpose [11]".

In the current scenario, there are many serious games concerning cybersecurity and were designed with the goal of teaching players about its main topics. Nevertheless, not always the balance between learning and gaming aspects is ensured leading to boredom and frustration feelings. For example, the serious game *Cybercity Chronicles*¹ allows players to learn basic cybersecurity concepts, but it has too many levels leading to the loss of interest. Other important aspects to include in the design of serious games are the user interface and the storyline, but not always they are considered. For instance, *Google XSS*² allows users to acquire a sufficient background in the field of cybersecurity, but the user interface is too minimal and it lacks of a storyline [12, 13].

To fill the existing gaps, in this research work a novel serious game for cybersecurity, called *Cyber Academy*, is presented and described. The game is being created following the iterative game design process which consists of four phases: planning, design and implementation, testing and evaluation [11]. This manuscript presents the planning and design phases while exploring the main characteristics and functionalities.

2. Cyber Academy: planning and design

Cyber Academy is a Serious Game for cybersecurity that aims to raise awareness with respect to the most important topics of this domain. By knowing the digital risks and threats to which an individual is subjected, it is easier to counter them and avoid being a victim of them. The target audience of *Cyber Academy* encompasses people aged in the range 16 to 60 years old with sufficient familiarity with computer science and medium-high reading skills. Concerning the technical aspects of the implementation of this serious game, it is planned to develop an application for mobile devices (i.e., smartphones and tablets).

Cyber Academy falls in the category of trivia games, in which the player is required to answer to some questions about different topics, and she/he must get as many correct answers as possible to win the game. This genre has been chosen because, the aim of the game is to enhance the players' awareness about basic cybersecurity topics while enjoying the learning activity [?] [14]. In this way, the balance between the learning and gaming aspects can be guaranteed.

2.1. Game Summary

The game flow outlines the major stages, interactions, and progression that players will experience. It will be organized in levels in which the player is allowed to learn cybersecurity concepts. More specifically, during the levels of the game, the player will interact with an avatar who will guide them along an educational path that include quizzes and minigames. When planning the development of any type of game, it is important to define its story, which refers to the narrative and the plot that provides a context, background, and purpose to the gameplay.

¹<https://www.sicurezza nazionale.gov.it/sisr.nsf/cybercity-chronicles.html>

²<https://xss-game.appspot.com/>

The story that Cyber Academy revolves around is set in the 21st century where chaos and cyber-crimes reign. The story features Blue and Red as protagonists; the characters are inspired by the role of the blue and red team in the real world. Blue is the champion of justice who helps and teaches victims how to fight cyber-crimes, while Red represents the red Team and is Blue's antagonist. During the game, the user is presented with numerous threats caused by Red, that has to face with Blue's help with the aim to make the world a safe place.

2.2. Aesthetics

The aesthetics refer to the visual and sensory elements that are included in the user interface and that influence the gaming experience. With the objective of recalling the standard cybersecurity colors, blue was chosen for the background because it represents the blue team that is responsible for the defense against the attacks.

2.3. Prototypes

According to the ISO 9241, prototypes are a representation of a product or a system that can be used for evaluation and further development purposes [15]. Figure 1 illustrates the horizontal prototype of Cyber Academy and is the preliminary step to the development by allowing to try multiple design solutions and adjust contents, titles, and button positions. This approach resulted to be useful in analyzing how the flow of the application translates into real-life interaction and use cases. In particular, the game allows players to choose the modality that they want to embark on: having a guided course from level 1 to level 5 or deciding to select the topic that they want to learn about, which happens in Step 2. Step 3-4 represent an example of how each level is structured: there are small explanations of cybersecurity concepts followed by challenges and quizzes. Depending the answers provided by the player, the behavior of the game changes: as illustrated in Step 4-6, wrong answers lead to further clarifications of the topic, while right answers are reinforced by congratulations and moving on to other concepts.

3. Educational Elements in Cyber Academy

The necessary informative resources for defining the educational elements of Cyber Academy are books, articles and similar apps.

3.1. Topics

The choice of the topics was based on an in-depth research of the literature and interviews with end users to understand the most addressed areas of cybersecurity in serious games and the current gaps.

Interviews were performed with the target users of Cyber Academy by asking them how much are familiar with technology and which is their knowledge about cyber threats.

Since this serious game is conceived for people who are not familiar with cybersecurity with respect to its technicalities, the topics range from basic notions to more complex topics [16]. The incremental cognitive difficulty was an intentional choice to keep the player engaged and to provide them with new challenges that are slightly more arduous, but affordable in terms of

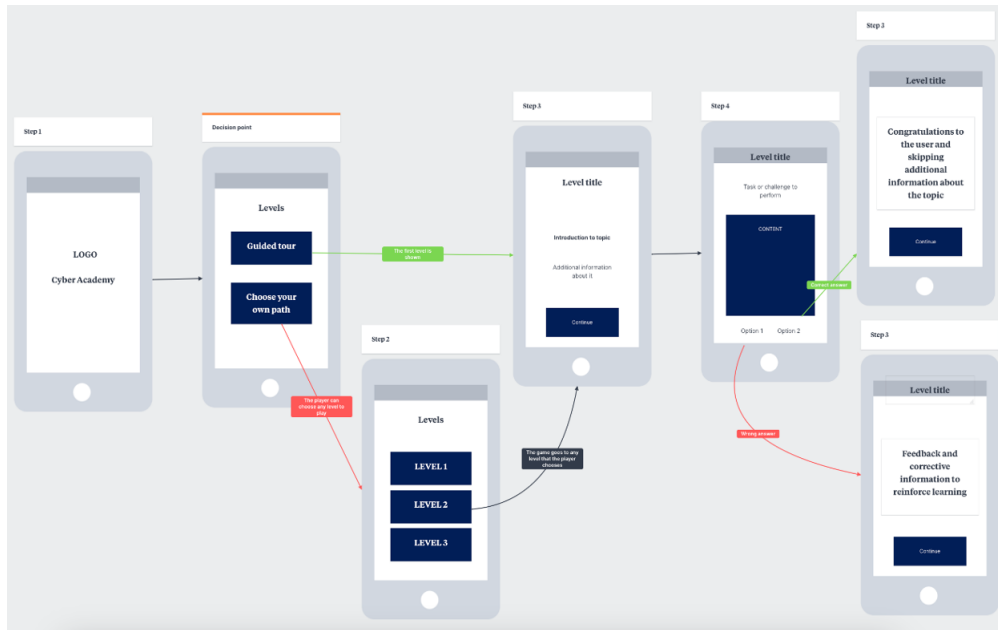


Figure 1: Horizontal prototype of Cyber Academy that illustrates the flow of the game

cognitive effort [17]. More specifically each topic is addressed by undertaking both a theoretical approach, providing definitions and a practical one by integrating exercises and challenges. At the current stage, it is intended to include the following topics:

- **Introduction To Cybersecurity:** this chapter aims at giving the player an overview of the basics of Cybersecurity, as in the concepts of attacks, threats, and assets [18].
- **Vulnerabilities:** the core of this chapter is to explain players what vulnerabilities are, which implications they have on people’s real lives and how they can be preventable [19].
- **Security:** this chapter is incredibly crucial for the game since the topic of the CIA triad is addressed [20].
- **Password and Privacy:** this topic was chosen because it is of widespread interest and affects everyone who benefits from any type of online service [21].
- **Attacks:** the most common types of attacks are involved, such as phishing, eavesdropping DDoS (Distributed Denial of Service), and malware [22, 20].

3.2. Skills

Putting players situations in which they need to dynamically act, make decisions, and evaluate situations is key for an effective learning process. The practical skills that Cyber Academy aims at teaching players are: to respond to critical situations; to create independently strong and secure passwords that are easy to remember; to be aware of their technological surroundings; to develop technical abilities in the field.

4. Conclusions and Future Works

Cybersecurity can be as intriguing as challenging when it comes to learning about it and all of its numerous characteristics. Serious games can represent a highly powerful tool to train individuals in this context.

This contribution presents Cyber Academy, a serious game for cybersecurity tailored to people who are not experts and that have basic knowledge and background experience in terms of daily technology usage. The objective lies in making people aware about how to face cyber-threats.

Future works of this research work involve integrating AI-powered chatbots giving users the impression that they are interacting with an entity with concrete speech skills, making the content of the conversation more relevant and memorable. This feature would reinforce the aspect of personalized learning fostering the symbiosis between the human and technology. In this way a smoother and realistic experience of use is provided to the end-users. Another future work may concern the integration of a database, in which users' information is stored, applying security and privacy patterns and rules, so that players can make use of a system that better suits their needs and to keep their progress saved. This would imply the use of external API and the construction of a domain to communicate with.

References

- [1] A. Pagano, M. Angelelli, M. Calvano, A. Curci, A. Piccinno, Quantum computing for learning analytics: An overview of challenges and integration strategies, in: Proceedings of the 2nd International Workshop on Quantum Programming for Software Engineering, QP4SE 2023, Association for Computing Machinery, New York, NY, USA, 2023, p. 13–16. URL: <https://doi.org/10.1145/3617570.3617867>. doi:10.1145/3617570.3617867.
- [2] V. S. Barletta, F. Cassano, A. Pagano, A. Piccinno, New perspectives for cyber security in software development: when end-user development meets artificial intelligence, in: 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), 2022, pp. 531–534. doi:10.1109/3ICT56508.2022.9990622.
- [3] C. C. Editor, Cybersecurity - glossary: Csrc, 2021. URL: <https://csrc.nist.gov/glossary/term/cybersecurity>.
- [4] M. T. Baldassarre, V. S. Barletta, D. Caivano, D. Raguseo, M. Scalera, Teaching cyber security: The hack-space integrated model, volume 2315, 2019.
- [5] M. T. Baldassarre, V. S. Barletta, D. Caivano, A. Piccinno, A visual tool for supporting decision-making in privacy oriented software development, in: Proceedings of the International Conference on Advanced Visual Interfaces, AVI '20, Association for Computing Machinery, New York, NY, USA, 2020. doi:10.1145/3399715.3399818.
- [6] V. Rossano, G. Calvano, Promoting sustainable behavior using serious games: Seadventure for ocean literacy, *IEEE Access* 8 (2020) 196931–196939.
- [7] M. M. Guala, A. Bikic, K. Bul, D. Clinton, A. Mejdal, H. N. Nielsen, E. Stenager, A. Søgaard Nielsen, “maze out”: a study protocol for a randomised controlled trial using a mix

- methods approach exploring the potential and examining the effectiveness of a serious game in the treatment of eating disorders, *Journal of Eating Disorders* 12 (2024) 35.
- [8] T. Anderson, G. Prue, G. McDowell, P. Stark, C. Brown Wilson, L. Graham Wisener, H. Kerr, G. Caughers, K. Rogers, L. Cook, et al., Co-design and evaluation of a digital serious game to promote public awareness about pancreatic cancer, *BMC Public Health* 24 (2024) 570.
- [9] F. Xiong, C. Drieschner, H. Wittges, H. Krcmar, Design and implementation of a serious game-teaching the interdependency between business models and business processes, in: *International Conference on Interactive Collaborative Learning*, Springer, 2023, pp. 503–514.
- [10] A. Yasin, L. Liu, T. Li, R. Fatima, W. Jianmin, Improving software security awareness using a serious game, *IET Software* 13 (2019) 159–169. doi:<https://doi.org/10.1049/iet-sen.2018.5095>.
- [11] G. Kalmpourtzis, *Educational game design fundamentals : a journey to creating intrinsically motivating learning experiences*, 1st ed., Taylor & Francis Group, 2019, p. 72.
- [12] V. Barletta, M. Calvano, F. Caruso, A. Curci, V. Rossano, Serious games for cybersecurity: Evaluating a design framework, in: *EDULEARN23 Proceedings, 15th International Conference on Education and New Learning Technologies, IATED, 2023*, pp. 4810–4815. URL: <https://doi.org/10.21125/edulearn.2023.1279>. doi:10.21125/edulearn.2023.1279.
- [13] V. S. Barletta, M. Calvano, F. Caruso, A. Curci, A. Piccinno, Serious games for cybersecurity: How to improve perception and human factors, in: *2023 IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRAINE), 2023*, pp. 1110–1115. doi:10.1109/MetroXRINE58569.2023.10405607.
- [14] F. Cassano, A. Piccinno, T. Roselli, V. Rossano, Gamification and learning analytics to improve engagement in university courses, in: T. Di Mascio, P. Vittorini, R. Gennari, F. De la Prieta, S. Rodríguez, M. Temperini, R. Azambuja Silveira, E. Popescu, L. Lancia (Eds.), *Methodologies and Intelligent Systems for Technology Enhanced Learning, 8th International Conference*, Springer International Publishing, Cham, 2019, pp. 156–163.
- [15] I. O. for Standardization, *Iso 9241:210 - ergonomics of human-system interaction: Human-centred design for interactive systems*, 2019. URL: <https://www.iso.org/standard/77520.html>.
- [16] R. Matovu, J. C. Nwokeji, T. Holmes, T. Rahman, Teaching and Learning Cybersecurity Awareness with Gamification in Smaller Universities and Colleges, in: *2022 IEEE Frontiers in Education Conference (FIE), IEEE, Uppsala, Sweden, 2022*, pp. 1–9. doi:10.1109/FIE56618.2022.9962519.
- [17] M. Salazar, J. Gaviria, C. Laorden, P. G. Bringas, Enhancing cybersecurity learning through an augmented reality-based serious game, in: *2013 IEEE Global Engineering Education Conference (EDUCON), IEEE, Berlin, 2013*, pp. 602–607. URL: <http://ieeexplore.ieee.org/document/6530167/>. doi:10.1109/EduCon.2013.6530167.
- [18] J. Pande, *Introduction to Cyber Security*, 2017.
- [19] P. Sangaronsilp, H. K. Dam, A. Ghose, On privacy weaknesses and vulnerabilities in software systems, in: *Proceedings of the 45th International Conference on Software Engineering, ICSE '23, IEEE Press, 2023*, p. 1071–1083. doi:10.1109/ICSE48619.2023.00097.
- [20] M. De Vincenzi, G. Costantino, I. Matteucci, F. Fenzl, C. Plappert, R. Rieke, D. Zelle, A

- systematic review on security attacks and countermeasures in automotive ethernet, *ACM Comput. Surv.* 56 (2024). URL: <https://doi.org/10.1145/3637059>. doi:10.1145/3637059.
- [21] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, S. Egelman, Of passwords and people: measuring the effect of password-composition policies, in: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '11*, Association for Computing Machinery, New York, NY, USA, 2011, p. 2595–2604. doi:10.1145/1978942.1979321.
- [22] G. Desolda, L. S. Ferro, A. Marrella, T. Catarci, M. F. Costabile, Human factors in phishing attacks: A systematic literature review, *ACM Comput. Surv.* 54 (2021). doi:10.1145/3469886.