

Article

An Educational Escape Room Game to Develop Cybersecurity Skills

Alessia Spatafora ¹, Markus Wagemann ², Charlotte Sandoval ³, Manfred Leisenberg ³
and Carlos Vaz de Carvalho ^{4,*} 

¹ Finance & Banking—Associazione per lo Sviluppo Organizzativo e delle Risorse Umane, Effebi Association, 00135 Roma, Italy; effebi@asseffebi.eu

² ASW Norddeutschland e.V., 22547 Hamburg, Germany; markus.wagemann@aswnord.de

³ Research & Development, Fachhochschule des Mittelstands, 33602 Bielefeld, Germany; charlotte.sandoval@fh-mittelstand.de (C.S.); manfred.leisenberg@fh-mittelstand.de (M.L.)

⁴ GILT R&D, Instituto Superior de Engenharia do Porto, 4249-015 Porto, Portugal

* Correspondence: cmc@isep.ipp.pt

Abstract: The global rise in cybercrime is fueled by the pervasive digitization of work and personal life, compounded by the shift to online formats during the COVID-19 pandemic. As digital channels flourish, so too do the opportunities for cyberattacks, particularly those exposing small and medium-sized enterprises (SMEs) to potential economic devastation. These businesses often lack comprehensive defense strategies and/or the necessary resources to implement effective cybersecurity measures. The authors have addressed this issue by developing an Educational Escape Room (EER) that supports scenario-based learning to enhance cybersecurity awareness among SME employees, enabling them to handle cyber threats more effectively. By integrating hands-on scenarios based on real-life examples, the authors aimed to improve the knowledge retention and the operational performance of SME staff in terms of cybersafe practices. The results achieved during pilot testing with more than 200 participants suggest that the EER approach engaged the trainees and boosted their cybersecurity awareness, marking a step forward in cybersecurity education.

Keywords: cybersecurity; serious games; escape rooms; educational games; small and mid-sized enterprises



Citation: Spatafora, A.; Wagemann, M.; Sandoval, C.; Leisenberg, M.; Vaz de Carvalho, C. An Educational Escape Room Game to Develop Cybersecurity Skills. *Computers* **2024**, *13*, 205. <https://doi.org/10.3390/computers13080205>

Academic Editor: Paolo Bellavista

Received: 23 June 2024

Revised: 12 August 2024

Accepted: 14 August 2024

Published: 19 August 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The frequency of cybercrime cases around the world has increased significantly in the recent years, together with the severity of their consequences. One of the reasons is the ongoing digitization of nearly all spheres of work and personal life, which has not been followed by the needed protective measures and has opened vulnerabilities to cyberattacks. For small and medium-sized enterprises (SMEs), attacks that tap into trade secrets or prevent the regular use of information, resources, or communication channels can mean economic ruin. As such, this rapid evolution of cyber threats requires SMEs to adopt robust cybersecurity measures to protect their online transactions and their sensitive data, to safeguard their operations and maintain customer trust [1]. SMEs must also navigate the complex landscape of legal and regulatory requirements, especially in the context of protecting not only their businesses, but also their customers' data and privacy [2]. But even when SMEs recognize the dangers of cyberattacks, they often lack comprehensive defense mechanisms, and/or they do not have the adequate resources or knowledge to implement them [3]. Yet, SMEs need proactive, informed, and strategic approaches to cybersecurity and must adopt scalable security measures that are adjusted to the rapidly changing cyber threat landscape [4–6]. Establishing tailored cybersecurity frameworks is crucial for SMEs to address their unique vulnerabilities and protect critical assets. Such

frameworks can help SMEs identify their sensitive data, assess the risks, and implement appropriate safeguards based on organizational needs and asset sensitivity [7].

Effective cybersecurity for SMEs involves not only adopting technological solutions, but also fostering a culture of security within the organization. So, it is highly important to inform employees about the effects and consequences of a cyberattack, to raise their awareness so that they engage in proactive risk management practices. Employees should receive in-house training at regular intervals so that the probability of a successful attack is limited and, in the event of an attack, adequate procedures are immediately taken. This training should be tailored to the specific needs and contexts of the SMEs, considering their resource constraints [8–11].

The EyesOnCS (enhancing cybersecurity through the development of training using an escape room model) project aimed to develop innovative solutions and concrete educational products to prepare current and future SME employees for working safely in the digital world. The main project result was a digital Educational Escape Room (EER) focused on cybersecurity that fostered active and experiential learning through a scenario-based learning approach depicting realistic situations from everyday work and life. The reason for choosing this method was the acknowledgement that this type of tool is gradually gaining attention within education and training as it provides an engaging approach that allows learners to efficiently achieve the predefined learning objectives [12,13]. Also, training with these tools allows learners to have a close reference to the working reality, which translates into higher knowledge retention and the immediate transfer/application of this knowledge to the workplace [14,15]. This learning approach gives the learners a self-managed and self-determined role as it is an active process of making choices, assessing options, observing the consequences, and reflecting on them. By acting and reacting to those situations, learners gain experience and develop their skills.

A large-scale testing and validation process with more than 200 participants was carried out in Germany, Italy, and Portugal with the engagement of the main target groups. After playing the game, participants provided feedback on their satisfaction and acceptance of the proposed methodology and tools, as well as their perception of the relevance and effectiveness of the approach.

2. Materials and Methods

Video games, which emerged as consumer products around half a century ago, have evolved significantly from their original form as leisure activities to become integral elements of social and cultural landscapes. The influence and presence of games in society have been steadily escalating, marking them as crucial components in various aspects of life. According to Goertz et al., these interactive mediums have transcended mere entertainment to embed themselves deeply within the fabric of modern culture [16]. Games, inherently endogenous systems, are composed of structured problem-solving activities governed by specific mechanics and rules. These elements collectively foster engagement, with players participating out of internal motivation. Gameplay dynamics and mechanics, the core of these systems, facilitate varied interactions between players and game elements, leading to diverse behaviors and outcomes which engender a sense of immersion, as well as a state of deep mental involvement that contributes significantly to critical thinking and logical reasoning. Furthermore, games are instrumental in honing other cognitive, intrapersonal, and interpersonal skills, including perceptiveness, attention, memory, and various analytical abilities [17].

Videogames have, since then, been repurposed beyond entertainment. Recognizing the motivational and engaging aspects of gameplay, designers have leveraged these attributes for educational and training purposes. These games, also known as “serious games”, are not primarily aimed at entertainment—they are committed to capitalizing on the inherent motivation and immersive experience of players, and use effective game mechanics to develop skills, knowledge, and/or awareness in an entertaining environment [18].

The education sector has achieved great success with the integration of these games (also referred to as educational games), which has led to the concept of “game-based learning” (GBL). For this purpose, games are designed with explicit learning objectives. As Prensky notes, GBL combines the engaging aspects of gaming with educational content, creating an interactive learning experience that motivates users to explore and deepen their knowledge [19]. Abt outlines the benefits of educational games and emphasizes the alignment of game objectives with educational goals; the promotion of the understanding of abstract concepts; the promotion of critical thinking; real-time feedback; and the provision of safe environments for the exploration of consequences and authentic assessment [20]. Educational games allow students to improve their social skills, teamwork, leadership, and collaboration. In addition, they are beneficial in training for hazardous processes (as is the case with cybersecurity applications and training) or situations where physical classrooms are too expensive. In short, the advantages of game-based learning can be summed up as follows:

- A playful addition to teaching methods, with a high motivation potential among learners through a sense of achievement in the game.
- Trackable active participation, widening the scope for action through interaction.
- Sustainable engagement with learning content.

Some of the disadvantages of game-based learning include the following:

- Learning content can be (partly) inferior.
- Requirements for technical equipment in some cases imply high costs.
- The games are very specific to a certain subject or domain.
- The teaching staff requires previous training [21].

Experiential learning, originally proposed by David Kolb as the process of learning by doing in a safe environment [22], provides the theoretical ground for game-based learning together with the active learning theory, proposed by Bonwell and Eison [23]. By engaging students in hands-on experiences and reflection, they become better able to connect theories and knowledge learned in the classroom to real-world situations. Educational Escape Room (EER) games are an experiential and active educational variety of the escape room game concept, targeted at the development of problem-solving, communication, collaboration, creativity, and critical thinking skills. Escape room games present an exciting narrative set in one or more fictional locations, such as prison cells, dungeons, laboratories, or even space stations, and the team of players is required to discover clues and solve puzzles aligned with the overall theme to achieve the final victory (normally escaping the room) within a limited time. The game normally begins with a brief introduction to the rules of the game, delivered by video, audio, or by a live gamemaster, and then players enter the room or area where they will be locked throughout the gameplay period. The game's challenges are generally more mental than physical, and different knowledge and skills are required for different types of puzzles. If players get stuck, there is normally a mechanism in place through which they can ask for hints that can be delivered in written, video, or audio form, or by the live gamemaster. Good endings are usually represented by escaping “alive” within the time limit (that is, completing the room's objective), while bad endings usually involve the players getting “killed” by the main driving force of the story or an antagonist coming to get the players once the timer has run out.

Virtual, digital, or online escape rooms are digital counterparts of physical escape rooms and take place through a computer and network. Like in physical escape rooms, the players solve riddles and complete puzzles within a limited amount of time. Escape room game software is used, which is either run by the players alone or by the gamemaster. This means that such games can be played by one player alone or by several players as a team. More complex digital escape rooms can use virtual reality to increase the sense of immersion of the players.

For some years now, the academic and vocational training sectors have recognized the benefits of escape rooms and have been using them for their own purposes. There are

already various scientific studies worldwide on the effectiveness and use of Educational Escape Rooms (EERs), although this is far from systematic, as shown by Tercanli et al. [24]. These studies show that EERs can be used in different phases of the learning process, so while some EERs do not require any prior knowledge and enable the basics to be learnt, others require prior knowledge and are designed to deepen that knowledge [25]. Both physical and virtual EERs are effective learning methods and show a significant increase in students' knowledge after the experience and a higher retention rate [26]. For instance, the Cyber Defense Tower Game allows players to defend servers from various cyberattacks, promoting strategic thinking and problem-solving skills [27]. Identically, the CyberHero game, which incorporates adaptive learning techniques, offers personalized experiences that can significantly improve user engagement and learning outcomes [28]. Similarly, the Cyber Secured game is designed for cybersecurity novices and has been shown to enhance learning and retention of cybersecurity concepts [29]. The CyberNEXS game provides a platform for simulating cyber challenges that cater to a wide range of users, from casual computer users to advanced cybersecurity professionals, illustrating the versatility of games in cybersecurity education [30]. The educational impact of cybersecurity games is further enhanced by their ability to simulate adversarial thinking, a critical component in cybersecurity training, as they can improve strategic reasoning by simulating hacker strategies [31]. Games can also be designed to boost interest in cybersecurity careers, especially among younger audiences. The GenCyber program demonstrates how games can increase awareness and interest in cybersecurity, potentially addressing the skills gap in this critical field [32]. The virtual escape room CySecEscape 2.0, designed to raise cybersecurity awareness among small and medium-sized enterprises, demonstrates how physical escape rooms can be successfully adapted into virtual environments without losing player immersion [33]. The escape room designed by the Institut National des Sciences Appliquées de Toulouse offers hands-on experience in recognizing and mitigating cyber threats, emphasizing the importance of choosing strong passwords and identifying phishing emails [34].

On the other hand, scenario-based learning (SBL) allows the integration of realistic situations from everyday working life into learning scenarios, according to the learning objectives. Scenario-based learning in combination with the EER game model is very effective for learning, as it can provide a realistic context together with an emotional connection, which increases motivation and accelerates the acquisition and retention of knowledge. The reference to realistic situations has a very positive learning effect, as students can better transfer the learned lessons to the working environment in a company. By using this approach, it is possible to provide scientifically evaluated and content-tested scenarios for educational purposes.

The adoption of this combination (EER + SBL) within the EyesOnCS project was expected to provide a better understanding of cybersecurity while increasing the engagement and the learning experience through interactive and emotional learning, as it...:

- Provides real-life experiences: Players are confronted with real-life experiences that may occur daily while working with a computer connected to the Internet. In addition, there is a convergence between the use of the Internet during work in the office and daily life.
- Provides immediate feedback on the consequences of online activities: During the game experience, the player can make their moves or decisions in a safe space where it is even possible to observe the direct consequences of various decisions. This makes it possible to gain experience and further information on the subject. The possible outcomes, such as identity theft, credit card fraud, etc., can be experienced in a game without real consequences.
- Ensures improved knowledge retention: game immersion and the immediate observation of eventual consequences lead directly to increased knowledge retention as the player/student is able to experience each choice and consequence during their playtime.

2.1. EyesOnCS Educational Escape Room

The EyesOnCS game was planned to be mostly oriented towards self-diagnostics and self-assessment in relation to cybersecurity, as it was mostly thought to be used in an informal, autonomous learning process by SME staff. In the scope of vocational training, the game can be used by VET trainers as an educational tool. But then, a formal assessment should be conducted through an external procedure.

Following a requirement study conducted with a set of SMEs and desk research analyzing a large number of cyberattacks, the specific learning objectives for the EyesOnCS EER were defined as:

- Expanding the knowledge of cyberattacks and cybercrime methods.
- Strengthening security awareness while dealing with Internet applications like e-mails, instant messengers, etc., on computers, smartphones, or any other connected devices.
- Acquiring knowledge of basic relevant behavioral principles and how these are used by cyber criminals, e.g., in social engineering.
- Strengthening physical awareness like the importance of the clean desk policy, information security, etc.
- Recognizing the important functions of social media while acknowledging its potential for use for criminal purposes.

These learning objectives were broken down in more detail by taking a closer look at the different attack methods identified from real cases of cybercrime, like phishing, password attacks, vishing, smishing, and social engineering. Something that all these attacks have in common is the exploitation of the so-called human factor, i.e., people who might commit mistakes out of ignorance or gullibility.

Phishing: Phishing is the most common attack method used by cyber criminals to gain access to other computer systems, and phishing mails are by far the number one attack method. The learning objectives regarding phishing for the project were:

- Building knowledge of typical phishing characteristics in emails.
- Understanding basic psychological principles used by criminals to deceive or manipulate people into not following security protocols.
- Raising awareness of the risk of unknown data attachments and the disclosure of personal data.
- Understanding the importance of clean desk policies and information security.
- Know how to get first aid and how to protect themselves.

Password attacks: Easy-to-guess passwords are, even today, one of the main reasons why accounts are so easily hacked. Easy passwords can be cracked by brute force attacks within seconds or less. Yet, the characteristics of a strong password are barely known in the public or workplace. To make the whole situation even more difficult, there is often misinformation circulating around passwords. Even the German Federal Office for Information Security advised a few years ago that it is important to change passwords on a regular basis. This advice fails to take two aspects into account. The first is that passwords are not like vegetables, so they cannot go bad that quickly. The second point is the general behavior of people when they need to change their passwords—whether they like it or not—as they tend to just swap out a few numbers, and passwords become easier to guess over time. The learning objectives for this vector attack were:

- Acquisition of basic knowledge about secure passwords.
- Understanding the principles of different methods for guessing, cracking, or otherwise obtaining passwords.
- Knowledge of clean desk policies.
- Understanding the basic principles of social engineering on social media to obtain passwords.
- Recognizing the importance of data that can be shared via social media.

Vishing: Voice phishing, or vishing, is a variation on the classic phishing email. These are phone calls made by psychologically trained criminals to obtain secret information over

the phone or to manipulate the victim into doing something that violates security protocols. Since AI voice generators became available, they have also been used to mimic the voices of CEOs to give orders over the phone. The learning objectives for vishing were:

- Understanding the basic principles of social engineering.
- Gaining awareness of suspicious calls and typical call patterns.
- Building knowledge of AI and voice generators.
- Obtaining general information about fraud.
- Gaining knowledge about measures for self-protection.

Smishing: Smishing is a variation of phishing and vishing. Attackers use instant messengers or text messages to involve the victim in a dialogue that is ultimately intended to lead to a demand for money via text, for example. This method is used in both professional and private environments and is one of the latest methods of attack in the world of cybercrime. The learning objectives for smishing are:

- Increasing the ability to recognize suspicious text messages.
- Acquiring the ability to check whether a text message is authentic or not.
- Developing the ability to protect oneself.

Social Engineering: Social engineering exploits psychological and behavioral aspects of human nature [35]. It involves deceiving or manipulating people into revealing sensitive information or performing actions that could jeopardize security. Almost every cybercrime attack method is accompanied or supported by social engineering capabilities. The learning objectives for social engineering are:

- Building knowledge about the topic in general.
- Raising awareness of dangerous messages, emails, and calls from unknown people.
- Acquisition of relevant basic psychological knowledge.

The chosen approach for the training process, together with the set of identified learning objectives, led to the decision to create a new game as none of the existing ones (namely those previously revised) covered all the goals and/or learning objectives, and their source code was not available; therefore, they could not be changed. The EyesOnCS game (Available at: <https://www.eyesoncs.eu/results>, accessed on 12 August 2024) follows a narrative where the player takes on the role of a new employee in the security department of a bank. During their work, they face various challenges related to the learning objectives previously described.

Episode 1—The Test: The first episode begins with the selection of an avatar and a name. To enter their new workplace, the player must enter an access code. They receive their first clue from the security guard at the door (Figure 1). The player must combine the letters used for the name of the bank, ECS (work place), with the alphabet to obtain the code with which they can enter the bank. This task gives some notions about the cryptographic process. After entering the bank, the player must set up their email account using their first password. Hints are provided around the desk and once the correct password has been used, the player can then select a new password. The player is asked whether the password should be saved on a computer and whether the anti-virus software should be switched off. The answer given then leads to further clues as to how the game could continue. The next task is to check certain emails to see whether they are possible phishing e-mails or not. The player can read and accept the emails as legitimate emails or reveal them as phishing e-mails. If the player identifies all e-mails correctly as legitimate or phishing e-mails, they will remain part of the game. If the player makes mistakes with the allocation of e-mails, they lose time, which might make it difficult to complete the EER. The episode ends with a summary of the topics learnt.



Figure 1. Starting the first episode.

Episode 2—The Job: The second episode begins with a relatively simple task for the player. The initial code for the building has been changed due to a hacker intervention. The player is given a hint about a specific date related to cybersecurity. After a quick Google search, the player can—with a little thought—enter the correct date as the new code. At their workplace, the player now receives several messages from colleagues that introduce them to the topics of phishing and vishing (Figure 2). The first e-mail leads to a suspicious fake website where the player has to find three typical markers for a fake website. Once the player has found these markers, they receive the next message. They are told to go to their colleague and leave their workplace. The player must now fulfil the clean desk policy (take their ID and smartphone with them, shut down their computer) before they can leave the workplace. The next scene in this episode is a phone conversation between the employee and their “supervisor” in which vishing markers are shown. It appears that the bank has been compromised. After the dialogue, the player receives a new phishing e-mail attempt (which they can also accept or reject). The next tasks focus on social media awareness, as the player must find three crucial pieces of information on their supervisor’s social media account. Here, they will have to find clues to the password the supervisor uses for his e-mail account.

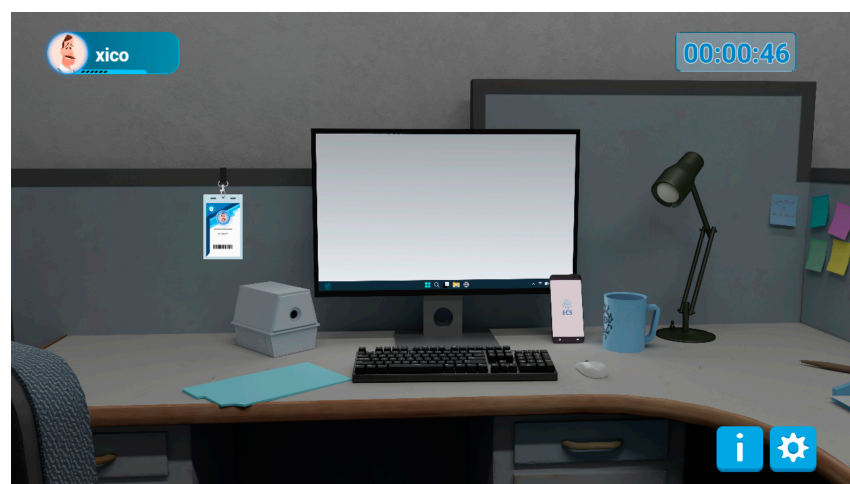


Figure 2. The player’s work environment in the bank.

Episode 3—The Hacker: The third episode is called “The White Hacker”. In this episode the player role-switches to a so-called “white hacker” story, so that the player can get to know the attacker’s point of view. The episode starts with the player receiving a message from the CEO of the ECS bank. He tells us that he knows why the player was fired

but he cannot do anything about it but he wants to use our expertise from the outside. As a white hacker he wants us to test the security of the bank systems. We accept the task and start investigating. The first job is to go to the Dark Web and find out what information is available about the company. We are able to retrieve the list of emails addresses of the company and phone numbers of the employees. With this information we prepare and start phishing and smishing campaigns for the employees. While the campaigns are running we start investigating the social media of the employees and realize that one of them posts a lot of information online. With that information we try to discover his access password. We contact again the CEO of the ECS bank and inform him that the information of the company is available on the Dark Web and that some accounts are hackable just by following the social media information of some employees. The CEO is then informed about the procedures he should adopt to make the bank systems secure. He is also informed about the importance of having a CSO (Chief Security Officer) that has full knowledge about cybersecurity.

Episode 4—The Expert: This is a quiz-based challenge that players can take at any moment. Therefore, it can be used for diagnostic purposes (if taken before playing a scenario) or for self-assessment if taken after playing a scenario. The questions for each round are randomly chosen from a large set of questions (more than 100 questions), which ensures that players have a different challenge every time they play it. Questions are associated with one or more of the three other episodes so that, if the player just finished one of those episodes and takes the quiz, the questions will be chosen from those associated with that episode.

2.2. Methodology

The validation of the game was done through a pilot testing process with primary objectives including assessing the educational value of the game, its playability, and its usability; identifying technical issues; and gathering user feedback to improve the game. The pilot testing lasted for three months (October to December 2023) and was conducted in three European countries: Germany, Italy, and Portugal. The participants were trainers and trainees from vocational schools and SME staff in those countries, as we had the intention of collecting data from both points of view. The selection of participants was done by project partners of organizations (schools and SMEs) that volunteered to participate and disseminated the information about the game internally. A hybrid implementation was adopted, combining face-to-face sessions (only in the schools) with the autonomous online playing of the game. In the face-to-face sessions, participants were informed about the project and game, they received a brief tutorial on the gameplay, and then they were able to play it themselves for about one hour. All participants were then allowed to play the game independently and autonomously after the session for about a week. In total, 384 participants were involved in the testing, as depicted in Figure 3.

On average, players spent 46 min playing the game (Figure 4), which shows the involvement of the players. Each scenario has a time limit of 30 min and the expected average play time for each scenario is about 20 min. This means that the players were involved, playing at least 3 scenarios on average.

Also, 84% of the players spent more than 1 min in the game, which shows that the number of “false testers” (that is, testers that just entered out of curiosity and immediately left) was quite reduced (Figure 5).

The total number of plays was 534, which means that each participant played the game between 1 and 3 times.

After playing the game, participants were asked to participate in an anonymous online survey. This meant that some players answered the questionnaire immediately after the face-to-face session, and others only answered it after one week. Unfortunately, due to the hybrid mode of the pilot testing, it was not possible to ensure that all the players did provide an answer so, in the end, only 77 participants provided feedback and comments.

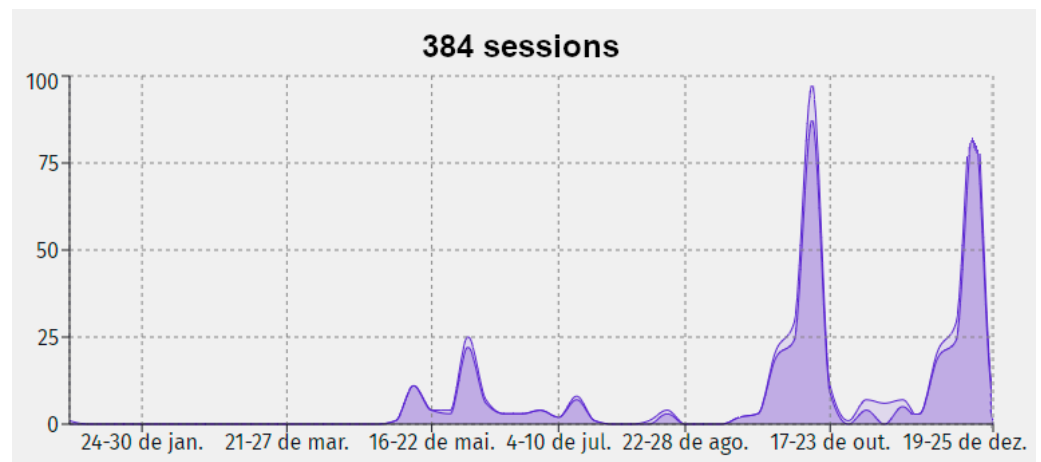


Figure 3. Game players throughout the entire testing period with special emphasis in pilot testing from October to December.

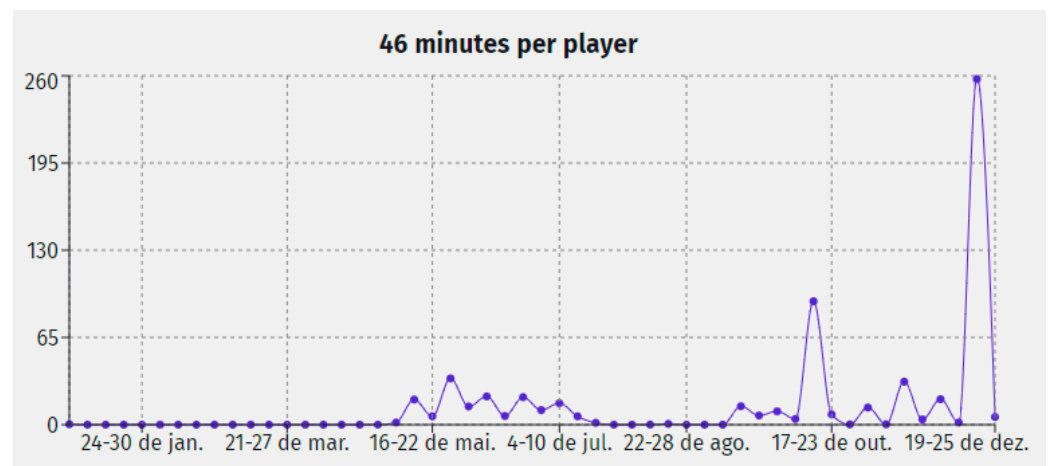


Figure 4. Average playing time during the same period.

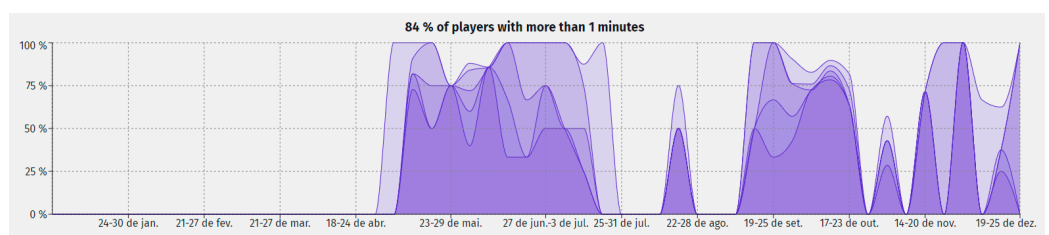


Figure 5. Players with more than 1 min of playing time during the same period.

3. Results

The questionnaire addressed some demographic aspects of the participants, as well as their perceptions of the usability, playability, and efficacy of the game.

Country of the respondents

- Portugal (5)
- Germany (23)
- Italy (12)
- Ukraine (7)—this group was part of the German pilot test.

The distribution of the players is slightly unbalanced between the different countries involved (more in Portugal and Germany, less in Italy) but, as there was no intention

of doing a country-based analysis, this distribution did not introduce any issues in the analysis of the results.

Age

- 10–20: 38
- 20–30: 16
- 30+: 23

The age distribution also roughly shows the difference between trainees and trainers/SME staff, which can be established as 1/3 and 2/3 of the total participants. This distribution was planned at the beginning of the project. In Italy, all the participants were younger than 30 years old, while all the Ukrainian participants were older than 30 years.

Sex

- Male: 46
- Female: 27

There was some predominance of male participants among the trainees (34 vs. 17), while for the older participants, the distribution was more balanced (13 vs. 10).

Professional occupation

- Trainer, teacher, equivalent (19)
- Student, trainee (51)
- Educational manager (3)
- Other (4)

These numbers reflect the distribution of students/trainees and teachers/trainers/SME staff that was also observed across the age categories. In Italy there was only one trainer and all the Ukrainian participants were either trainers or SME staff.

Usability of the game

Feedback on the usability of the game was collected using a standard System Usability Scale (SUS) questionnaire where participants quantified their agreement with a set of 10 statements [36]. Their answers were then normalized to the interval 1–5, with 1 representing strong disagreement and 5 representing strong agreement (Table 1).

Table 1. Usability of the game.

Statement	Score (1–5)
I think that I would like to use this game frequently.	3.82
I found the game unnecessarily complex.	2.12
I thought the game was easy to use.	3.68
I think that I would need the support of a technical person to be able to use this game.	2.12
I found that the various functions in this game were well integrated.	3.83
I thought there was too much inconsistency in this game.	1.96
I would imagine that most people would learn to use this game very quickly.	4.81
I found the game very cumbersome to use.	2.12
I felt very confident using the game.	3.71
I needed to learn a lot of things before I could get going with this game.	2.21
Final SUS score	76.7 (GOOD)

The SUS score is close to 80—this means that the usability of the game is GOOD according to the standard analysis, but close to VERY GOOD (ratio: 80). For the trainees, the SUS score was higher than the one reported by the trainers/SME staff (77.8 vs. 74.4),

although this difference is not significant and is expectable as they had more game-playing experience. Participants found the game easy to learn to use, with the functions well integrated, and they would use it frequently. They felt the need to learn a lot, which is connected to the learning nature of the game. Nevertheless, there are clearly some improvements to be made in relation to the usability and learning curve of the game.

Playability of the game

The playability of the game was analyzed using the standard Game Experience Questionnaire (GEQ) [37,38]. A set of 14 statements was used and players indicated their agreement with the statements through a Likert scale (5 levels), where 1 represented strong disagreement and 5 represented strong agreement (Table 2).

Table 2. Playability of the game.

Statement	Score (1–5)
I was interested in the game’s story	4.05
I felt successful	3.77
I felt bored	2.12
I found it impressive	3.29
I forgot everything around me	2.66
I felt frustrated	2.16
I found it tiresome	2.01
I felt irritable	2.04
I felt skillful	3.61
I felt completely absorbed	2.88
I felt content	3.60
I felt challenged	3.87
I had to put a lot of effort into it	3.82
I felt good	3.83

On the positive side, players were interested in the game’s story (4.05), they felt challenged (3.87), and felt good while playing the game (3.83). They did not feel bored, tired, or irritable. However, they were not totally absorbed by the game (2.85) to the point of forgetting everything around them (2.66). Older participants (trainers and staff) had a higher degree of interest in the game’s story (4.25 vs. 3.96), felt better playing the game (3.96 vs. 3.77), and felt much more absorbed (3.42 vs. 2.64). Younger players (trainees) did not feel irritable (1.89 vs. 2.38) or bored (2.00 vs. 2.38) and felt more successful (3.85 vs. 3.58). But in general, the differences between the two groups were not big.

Completing the game

Considering the participants that provided feedback, 59.7% (46) of them completed the game (completing the game meant that players went through the three scenarios and answered the quiz (one or more times)), which shows that most of the players were able to receive all the information and training about cybersecurity. Naturally, the other 31 participants (40.3%) did not finish the game, which means that they did not get through all the challenges and, therefore, were not able to acquire all the knowledge and skills. This was to be expected as this is a game and should be challenging, but there was a consensus that the hint system embedded in the game should be improved to ensure a higher finishing ratio. On average, players took 25 min to complete a scenario. Players that finished the game used five hints, on average, which was the expected number of hints for a smooth progression.

Players that did not finish the game considered it either too difficult (18) or too hard to understand how to play (4). Just a few considered it boring (2) or not interesting (1), which is a good ratio.

Qualitative feedback

Participants were asked to provide some qualitative comments about the game and the pedagogical methodology, and also some suggestions to improve the game. In relation to the game, the comments provided by the participants were very positive (in parenthesis are the number of participants that made a certain statement):

- A great idea, a positive game, it works very well (14).
- A very interesting game, I liked the challenges that made me think (7).
- I like the graphics but they can still be improved (4).
- I had fun (2).
- It was easy to use (2).
- A nice idea, it still needs some improvement but I would definitely use it with my students (2).
- The game was easy to use and I learned a lot. The part with the password was very interesting.
- I really liked the game but some puzzles are too difficult (9).
- Give more freedom to the player so that we do not need to follow a predefined path (3).
- More hints are needed at the beginning so you know what to do.

Equally positive feedback was received in relation to the learning process:

- I like the idea, it makes sense with our students, it is a nice and interesting way to learn (15).
- Very positive (13).
- Adequate and effective (7).
- I learned a lot about cybersecurity (7).
- It is interesting to have the learning outcomes. It explains what we have learned (2).
- I liked the learning approach with the riddles (2).
- I could use it in my classes to discuss concepts with my students (2).
- It works very well, I enjoy learning with games (2).
- It gave me some interesting guidance on creating a secure password. I think I will use the game's method in the future.
- It is cool to see that some of the points we made are useful for everyday use, and you remember the game if you are in a similar position at work.

4. Discussion

The SUS tool provided an overall score of 78.7, categorizing the game as “GOOD” and bordering on “VERY GOOD” (score 80). This high score suggests that users generally found the game easy to understand and use (4.81), with well-integrated functionalities (3.83). This indicates that the game's design facilitates a smooth learning curve and cohesive user experience. However, some users felt the game was complex (2.12) and would occasionally require technical support (2.12), suggesting areas where simplification could improve accessibility. The confidence levels in using the game were reasonably high (3.71), although there is still room for improvement to make the interface more intuitive.

The GEQ tool results offer insights into the emotional and cognitive aspects of the game experience. The game effectively engaged users, with high scores for story interest (4.05) and feeling challenged (3.87). This engagement is crucial for educational games where user interest directly impacts learning outcomes. Participants reported lower scores for feeling absorbed (2.88) and forgetting surroundings (2.66) which suggests that the game may struggle to maintain deep immersion, which could impact the sustained attention and learning. Positive emotional responses such as feeling successful (3.77) and good (3.83) outnumber negative reactions like frustration (2.16) and irritability (2.04), indicating a generally positive user experience.

About 59.7% of players completed the game, which is indicative of a well-balanced challenge level. However, the completion time was shorter than expected, and the hint system was noted as an area for potential improvement. Enhancements in these areas could lead to increased completion rates and deeper engagement.

User comments highlighted the educational value of the game, with many appreciating its challenge and the learning outcomes. Positive feedback emphasized the game's potential as a teaching tool in cybersecurity education. This follows the beliefs expressed by most of the literature sources, which agree that EERs can be valuable didactic learning methods and that they increase the students' interest in the topics covered, as they not only allow a deeper understanding of the course material already taught, but also help learners to understand connections between these topics [24]. Furthermore, EERs have been shown to positively influence confidence not only in academics, but also in the operational application of what has been learnt, as they can help students see a broader picture of course material by enhancing their understanding of additional interrelationships between topics [24–34].

5. Conclusions

Overall, the game was well received, with substantial strengths reported for usability, player engagement, and educational value. Improvements in game depth, immersion, and interface simplicity could further enhance its effectiveness. This feedback serves as a valuable guide for future development, ensuring the game not only entertains, but also educates effectively in the realm of cybersecurity.

As stated in the reviewed literature, the escape room approach promotes soft skills in general, increasing motivation and improving skills such as problem solving, as demonstrated by the studies of Veldkamp et al., and Fotaris and Mastoras [12,39]. Team building, out-of-the-box thinking, and critical questioning are also enhanced with EERs, as shown by Cain, Clarke and Peel, and Eukel [40–42]. In addition to this, learning with the escape room approach also creates an awareness of a specific topic or domain [43].

This is particularly desirable for the EyesOnCS project, which aims to support awareness of the responsible handling of cybersecurity issues. The escape room approach demonstrates significant pedagogical value, aligning with research that supports its use as an effective educational method. The game's ability to engage users with its high story interest score and the feeling of being challenged is crucial in educational settings, where sustained engagement directly impacts learning outcomes. By integrating these elements, the game encouraged active participation and problem-solving, which are essential for effective learning. Participants' feedback highlighted the educational benefits of the game, the game's challenges, and the depth of learning outcomes, reinforcing its potential as a teaching tool. This positive response is consistent with the aforementioned literature, which suggests that escape rooms can significantly increase students' interest in topics by allowing them to explore course material in a dynamic and interactive way. Such an approach not only deepens understanding, but also helps students identify connections between different topics, promoting a more holistic view of the subject matter.

Moreover, based on the qualitative comments received, the game positively influenced learners' confidence levels in the practical application of cybersecurity knowledge. By providing a platform for players to see the broader picture and understand the interrelationships between topics, the game fosters a deeper comprehension and higher retention of information. This aligns with studies indicating that Educational Escape Rooms enhance students' ability to apply learned concepts in real-world scenarios, thereby bridging the gap between theoretical knowledge and practical skills.

Overall, the EyesOnCS EER game represents a promising pedagogical approach, offering a unique blend of challenge, engagement, and educational value that can effectively enhance learning experiences.

Author Contributions: Conceptualization, A.S. and M.L.; methodology, M.L. and C.V.d.C.; software, C.V.d.C.; validation, A.S., M.L., M.W. and C.V.d.C.; formal analysis, C.V.d.C.; investigation, C.S.; data curation, C.S.; writing—original draft preparation, C.S.; writing—review and editing, C.V.d.C.; supervision, C.V.d.C.; project administration, M.L.; funding acquisition, M.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was co-funded by the European Union through the Erasmus+ Programme, grant number 2021-1-DE02-KA220-VET-000033003.

Data Availability Statement: The research data can be obtained by contacting the authors.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Saleem, J.; Adebisi, B.; Ande, R.; Hammoudeh, M. A state of the art survey—Impact of cyber attacks on SME's. In Proceedings of the International Conference on Future Networks and Distributed Systems, Cambridge, UK, 19–20 July 2017. [\[CrossRef\]](#)
2. Kasl, F. Cybersecurity of Small and Medium Enterprises in the Era of Internet of Things. *Lawyer Q.* **2018**, *8*, 165–188.
3. Wallang, M.; Shariffuddin, M.; Mokhtar, M. Cyber Security in Small and Medium Enterprises (SMEs). *J. Gov. Dev. (JGD)* **2022**, *18*, 75–87. [\[CrossRef\]](#)
4. van Tooren, M.; Reti, D.; Schneider, D.; Bassem, C.; de la Cámara, R.S.; Schotten, H.-D. Research Questions in the Acceptance of Cybersecurity by SMEs in the EU. In Proceedings of the Computer Safety, Reliability, and Security—SAFECOMP 2022, Munich, Germany, 6–9 September 2022; pp. 247–255.
5. Manzoor, J.; Waleed, A.; Fareed Jamali, A.; Masood, A. Cybersecurity on a Budget: Evaluating Security and Performance of Open-Source SIEM Solutions for SMEs. *PLoS ONE* **2024**. Available online: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0301183> (accessed on 8 April 2024). [\[CrossRef\]](#)
6. Erdogan, G.; Halvorsrud, R.; Boletsis, C.; Tverdal, S.; Pickering, J. Cybersecurity Awareness and Capacities of SMEs. In Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023), Lisbon, Portugal, 22–24 February 2023; pp. 296–304. [\[CrossRef\]](#)
7. Ajmi, L.H.; AlQahtani, N.; Rahman, A.; Mahmud, M. A Novel Cybersecurity Framework for Countermeasure of SME's in Saudi Arabia. 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 1–3 May 2019; pp. 1–9. [\[CrossRef\]](#)
8. Pieczywok, A. Training employees on risks in the area of cybersecurity. *Cybersecur. Law* **2022**, *7*, 261–271. [\[CrossRef\]](#)
9. Corradini, I. *Building a Cybersecurity Culture in Organizations*; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; pp. 63–86. [\[CrossRef\]](#)
10. Tolossa, D. Importance of cybersecurity awareness training for employees in business. *Vidya* **2023**, *2*, 104–107. [\[CrossRef\]](#)
11. Trim, P.; Upton, D. *Cyber Security Culture: Counteracting Cyber Threats through Organizational Learning and Training*, 1st ed.; Routledge: London, UK, 2016. [\[CrossRef\]](#)
12. Veldkamp, A.; van de Grint, L.; Knippels, M.-C.; van Joolingen, W. Escape education: A systematic review on escape rooms in education. *Educ. Res. Rev.* **2020**, *31*, 100364. [\[CrossRef\]](#)
13. Pornsakulpaisal, R.; Ahmed, Z.; Bok, H.; Carvalho Filho, M.A.; Goka, S.; Li, L.; Patki, A.; Salari, S.; Sooknarine, V.; Woon Yap, S.; et al. Building Digital Escape Rooms for Learning: From Theory to Practice. The Clinical Teacher. Available online: <https://asmepublications.onlinelibrary.wiley.com/doi/full/10.1111/tct.13559> (accessed on 8 April 2024).
14. Acharya, S.; Maxim, B.; Yackley, J. Applied Knowledge Retention—Are Active Learning Tools the Solution? In Proceedings of the 2019 ASEE Annual Conference & Exposition, Tampa, FL, USA, 16–19 June 2019. [\[CrossRef\]](#)
15. Chen, M. Research on the Relationship between Training and Knowledge Worker Retention. *DEStech Trans. Soc. Sci. Educ. Hum. Sci.* **2016**. [\[CrossRef\]](#) [\[PubMed\]](#)
16. Goertz, L.; Fehling, C.; Hagenhofer, T. Didaktische Konzepte Identifizieren—Community of Practice zum Lernen mit AR und VR. In Proceedings of the Social Virtual Learning; 2020; p. 3. Available online: https://www.social-augmented-learning.de/wp-content/downloads/210225-Coplar-Leitfaden_final.pdf (accessed on 8 April 2024).
17. Vaz de Carvalho, C.; Coelho, A. Game-Based Learning, Gamification in Education and Serious Games. *Computers* **2022**, *11*, 36. [\[CrossRef\]](#)
18. Baptista, R.; Coelho, A.; Vaz de Carvalho, C. Relationship between game categories and skills development: Contributions for serious game design. In Proceedings of the European Conference on Game Based Learning, Steinkjer, Norway, 8–9 October 2015; Volume 1, pp. 34–42.
19. Prensky, M. *Digital Game-Based Learning*; McGraw-Hill: New York, NY, USA, 2001; Volume 1, p. 1. [\[CrossRef\]](#)
20. Abt, C. *Serious Games*; University Press of America: Lanham, MD, USA, 1987.
21. Pohl, M.; Rester, M.; Judmaier, P. Interactive Game Based Learning: Advantages and Disadvantages. In *Universal Access in Human-Computer Interaction. Applications and Services. UAHCI 2009. Lecture Notes in Computer Science*; Stephanidis, C., Ed.; Springer: Berlin/Heidelberg, Germany, 2009; Volume 5616. [\[CrossRef\]](#)
22. Kolb, D. *Experiential Learning: Experience as the Source of Learning and Development*; Prentice Hall: Englewood Cliffs, NJ, USA, 1984.

23. Bonwell, C.C.; Eison, J.A. *Active Learning: Creating Excitement in the Classroom*. ASH#-ERIC Higher Education Report No. 1; The George Washington University, School of Education and Human Development: Washington, DC, USA, 1991.
24. Tercanli, H.; Martina, R.; Ferreira Dias, M.; Reuter, J.; Amorim, M.; Madaleno, M.; Magueta, D.; Vieira, E.; Veloso, C.; Figueiredo, C.; et al. *Educational Escape Rooms in Practice: Research, Experiences and Recommendations*; UA Editoria: Tucson, AZ, USA, 2021. [\[CrossRef\]](#)
25. Guckian, J.; Sridhar, A.; Meggitt, S.J. Exploring the perspectives of dermatology undergraduates with an escape room game. *Clin. Exp. Dermatol.* **2020**, *45*, 153–158. [\[CrossRef\]](#) [\[PubMed\]](#)
26. Brady, S.; Andersen, E. An escape-room inspired game for genetics review. *J. Biol. Educ.* **2019**, *55*, 406–417. [\[CrossRef\]](#)
27. Jin, G.; Tu, M.; Kim, T.; Heffron, J.; White, J. Game based Cybersecurity Training for High School Students. In Proceedings of the 49th ACM Technical Symposium on Computer Science Education, Minneapolis, MN, USA, 27 February–2 March 2018. [\[CrossRef\]](#)
28. Hodhod, R.; Hardage, H.; Abbas, S.; Aldakheel, E. CyberHero: An Adaptive Serious Game to Promote Cybersecurity Awareness. *Electronics* **2023**, *12*, 3544. [\[CrossRef\]](#)
29. Kletenik, D.; Butbul, A.; Chan, D.; Kwok, D.; LaSpina, M. Cyber Secured: A Serious Game for Cybersecurity Novices. In Proceedings of the 51st ACM Technical Symposium on Computer Science Education, Portland, OR, USA, 11–14 March 2020. [\[CrossRef\]](#)
30. Nagarajan, A.; Allbeck, J.; Sood, A.; Janssen, T. Exploring game design for cybersecurity training. In Proceedings of the 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), Bangkok, Thailand, 27–31 May 2012; pp. 256–262. [\[CrossRef\]](#)
31. Hamman, S.; Hopkinson, K.; Markham, R.; Chaplik, A.; Metzler, G. Teaching Game Theory to Improve Adversarial Thinking in Cybersecurity Students. *IEEE Trans. Educ.* **2017**, *60*, 205–211. [\[CrossRef\]](#)
32. Jin, G.; Tu, M.; Kim, T.; Heffron, J.; White, J. Evaluation of Game-Based Learning in Cybersecurity Education for High School Students. *J. Educ. Learn.* **2018**, *12*, 150–158. [\[CrossRef\]](#)
33. Löffler, E.; Schneider, B.; Zanzwar, T.; Asprion, P.T. CySecEscape 2.0—A Virtual Escape Room to Raise Cybersecurity Awareness. *Int. J. Serious Games* **2021**, *8*, 59–70. [\[CrossRef\]](#)
34. Beguin, E.; Besnard, S.; Cros, A.; Joannes, B.; Leclerc-Istria, O.; Noel, A.; Roels, N.; Taleb, F.; Thongphan, J.; Alata, E.; Nicomette, V. Computer-Security-Oriented Escape Room. *IEEE Secur. Priv.* **2019**, *17*, 78–83. [\[CrossRef\]](#)
35. Salahdine, F.; Kaabouch, N. Social Engineering Attacks: A Survey. *Future Internet* **2019**, *11*, 89. [\[CrossRef\]](#)
36. Brooke, J. SUS: A quick and dirty usability scale. In *Usability Evaluation in Industry*; CRC Press: Boca Raton, FL, USA, 1995; p. 189.
37. IJsselstein, W.A.; de Kort, Y.A.W.; Poels, K. *The Game Experience Questionnaire*; Technische Universiteit Eindhoven: Eindhoven, The Netherlands, 2013.
38. Law, E.L.-C.; Brühlmann, F.; Mekler, E.D. Systematic Review and Validation of the Game Experience Questionnaire (GEQ)—Implications for Citation and Reporting Practice. In Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play, Melbourne, Australia, 28–31 October 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 257–270.
39. Fotaris, P.; Mastoras, T. Escape rooms for learning: A systematic review. *Res. Pract. Technol. Enhanc. Learn.* **2019**, *14*, 235–243.
40. Cain, J. Exploring the benefits of using gamification and video games for adult learners. *J. Contin. High. Educ.* **2019**, *67*, 45–54.
41. Clarke, S.; Peel, D. Escape the norm! Using escape room activities to support experiential learning in undergraduate business education. *Int. J. Manag. Educ.* **2020**, *18*, 100425.
42. Eukel, H.N.; Frenzel, J.E.; Cernusca, D. Educational gaming for pharmacy students—Design and evaluation of a diabetes-themed escape room. *Am. J. Pharm. Educ.* **2017**, *81*, 6265. [\[CrossRef\]](#)
43. Adams, V.; Burger, S.; Crawford, K.; Setter, R. Can you escape? Creating an escape room to facilitate active learning. *J. Nurses Prof. Dev.* **2018**, *34*, 60–63. [\[CrossRef\]](#) [\[PubMed\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.