International Journal of Serious Games

ISSN: 2384-8766
https://journal.seriousgamessociety.org/

Article

Serious Games to Improve Privacy and Security Knowledge for Professionals: a Systematic Literature Review

Chaimae Moumouh[1], José A. García-Berná[2], Mohamed Yassin Chkouri[1], José L. Fernández-Alemán[2]

[1] *SIGL Laboratory, ENSATE, Abdelmalek Essaadi University, Tetouan, Morocco*
[2] *Department of Computer Science and Systems, University of Murcia, Spain*
chaimae.moumouh@etu.uae.ac.ma; josealberto.garcia1@um.e; mychkouri@uae.ac.ma; aleman@um.es

Keywords:

Serious games
Gamification
Privacy
Security
Systematic literature review,
Survey

Received: June 2024
Accepted: January 2025
Published: February 2025
DOI: 10.17083/ijsg.v12i1.825

Abstract

This study explores the use of serious games (SGs) for teaching information security and privacy, focusing on their effectiveness in raising cybersecurity awareness among employees. A systematic literature review (SLR) was conducted, guided by nine research questions: the publication trends, environments, intellectual property, game genres, mechanics, player profiles, and the effectiveness of SGs in improving employees' cybersecurity knowledge. Which identified 17 relevant publications from an initial pool of 1,737 articles. The publications were analyzed based on factors such as publication trends, game scope, genres, mechanics, and player profiles. The findings indicate that while SGs have potential in improving security awareness, most of the identified games are in early development and testing stages, often involving small participant groups. A notable gap was found in the availability of SGs tailored for specialized sectors, especially healthcare, despite the growing need for security awareness in this field. This study contributes to the state of the art by highlighting this gap and calling for further development of SGs in critical sectors. The originality lies in identifying this underexplored area, providing a foundation for future research and development of more effective SGs for sector-specific cybersecurity training.

1. Introduction

The adoption of gamification is of great interest in information systems. Moreover, this field has experienced tremendous popularity and growth since the last decade [1]. Several definitions of gamification can be encountered in the literature. The simplest one that can be given to this term is: "gamification is the use of game design elements in non-game contexts" [2]. Gamification's main goal is to apply gaming techniques in various areas, such as health, social life and business [3, 4]. Gamification has several advantages such as promoting

engagement, challenging the creativity of users, and execution when completing a specific task [5]. Gamification employs the features that make games exciting, engaging, and unexpectedly addicting to boost the player experience in non-game contexts like the workplace or education [6]. However, the aforementioned definition is related to another concept, serious games [7]. In the most traditional meanings of SGs, they are viewed as "games that do not have entertainment, enjoyment or fun as their primary purpose", or "games that are designed to entertain players as they educate, train or change behavior" [8]. SGs are important in fields such as education, military, economics, health, and politics [9]. Even though SGs and gamification might seem very similar, and will in general be used for purposes other than their normal diversion use, their executions vary extensively [10]. Sometimes SGs referred to as "games with a purpose" provide exclusive gaming experiences via rules, engines, and game mechanisms, Gamification aims to generate gaming-like experiences using a variety of game mechanics and game experience design [9]. Previous research [11] has demonstrated the effectiveness of gamification, particularly in enhancing engagement, and interest, and promoting positive behavior change. The study conducted a systematic literature review (SLR) addressing knowledge gaps in the application of gamification for cybersecurity awareness among non-IT professionals and students. While serious games and gamification aim to foster engagement and learning, they are distinct concepts: gamification involves integrating game-like elements into non-game contexts, whereas serious games are complete, purpose-built games designed to achieve specific learning outcomes. Building on this distinction, our research shifts the focus from gamification to serious games, aiming to address knowledge gaps in their application for improving privacy and security knowledge.

The main purpose of our study is to conduct a systematic literature review (SLR) on the use of SGs to teach employees about the privacy and security of information. A profound analysis has been carried out to offer a systematic perspective of the current status of literature in the field and to define any flaws or gaps that may exist. This study is driven by the need to explore how serious games (SGs) can be used to teach information security and privacy. Through a systematic literature review (SLR), we aim to answer nine key research questions, ranging from the publication trends of SGs (RQ 1) to their effectiveness in improving employee security awareness (RQ 9). This research also highlights a critical gap in the availability of SGs tailored to specialized fields, such as healthcare, an area that demands heightened security awareness. Furthermore, the possible impacts and challenges of incorporating gaming aspects into data breach solutions were discussed. The body of the paper is organized as follows: Section 2 explains how the systematic literature review was developed; in Section 3, the findings of this research were given, including answers to the research questions; Section 4 discusses the study's results; and Section 5 includes the paper's conclusions and offers issues that may lead to further research.

2. Materials and Method

Before elaborating on any particular research issue, subject area, or phenomenon of interest, a literature review is essential [12]. An SLR is a method of discovering and analyzing a collection of related literature to identify gaps to investigate in a specific topic [13]. An SLR helps to gain a better insight and understanding of the existing work by evaluating relevant articles to identify existing shortcomings, to test a theory and/or build new hypotheses. When performing an SLR, specific steps were carried out. First, research questions were defined, second, a research protocol was developed, thirdly the literature search was performed, fourth, we started the data extraction, and then a quality evaluation

was conducted. Next, the data and results retrieved were analyzed and finally, an interpretation of results was performed [14].

2.1 Research questions and search protocol

An efficient SLR involves precise research questions, to achieve the purpose of the study. Table 1 lists the nine identified research questions for this literature review and the corresponding rationale for each one. The literature search was conducted using popular scientific digital libraries: Scopus, ScienceDirect, Wiley InterScience (subject Computer Science), ACM Digital Library, IEEE-Xplore, Springer Database, and PubMed. To conduct searches in the chosen digital libraries, and to make sure that the entire scope of the study is covered, a search string has been structured and divided into three parts as presented in Table 2. The major parts were combined using the Boolean ”AND”, as for the terms belonging to the same concept they were joined with the Boolean ”OR”. To extract the papers, the search term was applied to the metadata (title, keywords, and abstract) in each digital library.

Table 1. Research mapping questions & rationale

Question	Rationale
1. How has research on the use of SGs to earn about security and privacy been dissemi nated through time and between countries? 2. Which journals are the main targets of articles on SGs to practice data security and privacy? 3. What are the environments of SGs?	o determine the geographical and temporal evolution of publications concerning SGs as training tools. To identify the most prolific sources in which articles related to this topic are being published. To identify the adopted environment (standalone, mobile, web, non-digital) of these SGs. Investigating the environments of SGs is crucial for gaining insights into the contexts, settings, and conditions under which SGs are employed. By understanding the environments, researchers can analyze factors such as the target audience, technological infrastructure, educational or training contexts, social or cultural influences, and more.
4. What SGs have a pricing and intellectual property?	To identify to whom (recognized companies, academic institutions, or others) belong the intellectual property rights of these SGs, the forms of distribution of these SGs if a license is applicable, and the pricing strategies (free/paid) of these SGs. Researchers can gain insights into the market viability and business strategies employed by SG developers in this domain. This understanding can be valuable for stakeholders, such as organizations seeking to invest in or adopt these training solutions.
5. What are the focus and scope of SGs?	In this question, the focus (professional/academic) of these SGs, is identified along with their public and market. By investigating the focus, researchers can delve into the educational, behavioural, or cognitive aspects that SGs intend to address. Additionally, exploring the scope allows for analyzing the breadth of topics, domains, or skills covered by SGs.
6. What game genres are the most/least popular among SGs for healthcare?	To identify the aim to assess the popularity of game genres among SGs, by grouping the latter by their game genre following the classification by Lameras et al. [15]. By exploring the popularity of game genres among SGs in this domain, researchers can gain insights into which genres are considered more effective in engaging learners, fa-

	cilitating knowledge retention, and improving cyber security skills.
7. What are the game-related approaches implemented in the SGs?	In this question, we identify both the gamification elements along side with the game mechanics implemented in SGs. Gamification elements are identified following the periodic table of gamification elements proposed by Marczewski [16] while game mechanics are extracted from the LM-GM framework [17].
8. What type of characters are included in the SGs and to what extent do SGs achieve a deep knowledge of the player?	To identify what type of characters have included and what kind of player profiles have been addressed in SGs, highlight the characteristics of the player profiles identified and investigate to what extent does SGs adapt the gameplay to match the player profiles.
9. What evaluation studies have been carried out with those SGs ?	Information on how the found SGs were evaluated, this can include effectiveness, design, performance and engagement.

Table 2. Search string

Scope	String
Gamification	(”serious game”
	AND
Training	”training”
	AND
Privacy and security	(”cybersecurity” OR ”security” OR ”privacy”))

2.2 Inclusion and exclusion criteria

To review and choose the most relevant studies among those discovered, a combination of inclusion and exclusion criteria was established, after removing the duplicates. The selection procedure was handled by the authors, which took into account the data in the articles and by reviewing the whole papers. The studies published online in the time frame 2006 to 2021 that satisfied at least one of the following criteria were included:

- **IC**1. The article describes the application of SGs to learn about security and privacy.
- **IC2.** The paper offers experimental evidence on the influence of SGs on improving professionals’ security and privacy knowledge.

The following exclusion criteria were used to discard papers not suitable for our study. If at least one of these exclusion criteria is met, the paper is withdrawn:

- **EC1.** Publications published prior to 2006 or after December 31, 2021
- **EC2.** Papers not written in English.
- **EC3.** Only abstracts or PowerPoint slides were accessible for the literature.
- **EC4.** Papers that discuss the application of SGs in the domain of security and privacy awareness, for users other than employees as well as those that do not give sufficient information or study on the subject.
- **EC5.** The paper lies outside the SGs to learn about security and privacy.

2.3 Quality assessment

All the retrieved articles went through a quality assessment performed by the authors, in the form of a set of closed questions in order to prevent any possible unfairness in the exclusion of papers during the systematic literature review, and assess the relevance of the studies. A previous study [18] was used to identify the following five quality assessment questions:

- **QA1.** Does the paper discuss in details the game elements or the SGs mechanics employed in the study?
  The available choices were "Yes (+1)", No "(+0)" and "Partially (+0.5)".
- **QA2.** Is the study's outcome tested and proven?
  The available choices were "Yes (+1)" and No "(+0)".
- **QA3.** Is there any discussion of the advantages and benefits of SGs in the paper?
  The available choices were "Yes (+1)" and No "(+0)".
- **QA4.** Do the authors address the restrictions or limitations of SGs?
  The available choices were "Yes (+1)" and No "(+0)".
- **QA5**. Is the work published in a conference proceedings or relevant journal?

2.4 Data extraction strategy and synthesis method

To conduct out a comprehensive literature study and answer the research questions posed, a structured sheet was used which contained the necessary data to extract for each of the articles selected. The extracted data is described below.

- **RQ 1:** The date of publication and nationalities of the authors.
- **RQ 2:** Each article's source and channel.
- **RQ 3:** The different environments of SGs.
- **RQ 4:** The pricing and intellectual property of the SGs developed by authors.
- **RQ 5:** The scope and focus of the SGs.
- **RQ 6:** The game genres on existing SGs.
- **RQ 7:** The used game mechanics and elements.
- **RQ 8:** The player profiles.
- **RQ 9:** Results proving the effectiveness of SGs on improving employees' security and privacy knowledge.

One author independently reviewed initially titles and then abstracts, to decide if an article should be included or excluded based on the criteria mentioned above. The included original research publications should address SGs created for professionals to raise their security and privacy knowledge and awareness, such as games that teach professionals how to manipulate and handle patients' data correctly to avoid human errors. Throughout the title and abstract review process, the authors attained a level of agreement on inclusion and exclusion. All full-text publications were evaluated for selection, and all papers that were rejected were reported. To address the research questions, the information acquired from the most relevant studies was synthesized. The findings are reported using descriptive statistics and are visually depicted to aid comprehension.

3. Results and Discussion

The findings to respond to the research questions listed in Table 1 are described in this section. Between October and November 2022, the selection procedure was carried out. Using the previously mentioned search criteria, a total of 1736 publications were returned from the database searches, as shown in Fig. 1. After eliminating duplicates and publications

that satisfied the first three exclusion criteria, those published before January 2006 and after December 2021 as well as the papers that were not written in English, a screening based on their metadata, was conducted on the remaining documents (title, keywords and abstract). Following the application of IC1, IC2, and EC4, 1039 were eliminated. The entire texts of the remaining 77 papers were taken into account when evaluating them. After using EC5, 60 papers were eliminated, and 17 articles concentrating on SGs in raising privacy and security awareness were chosen. Thus, our systematic literature review finally contained a total of 17 studies.

Table 3. list of selected SGs along with their references, sources and environment

SGs	Ref.	Sources	Environment
InfoSecure	[36]	International Journal of Advanced Computer Science and Applications	Web-based(The game can run on PC, smartphones, and browsers)
NHSGGC	[30]	International Journal of SGs	Not provided
Role-playing quiz application (RPG)	[28]	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	Mobile-based application on Android platform
Riskio	[29]	Computers & Security	Card game (Non-digital)
Another week at the office (awato)	[31]	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	Not provided
CyberCIEGE	[37]	Computers & Security	Web-based
The CyberSecurity Awareness Quiz	[27]	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	Online
Cyber Security Requirements Education Game (SREG)	[42]	Information and Software Technology	Card game (Non-digital)
SIRET Security Game	[32]	Journal of Visual Languages & Computing	The game is exported as a SCORM package, allowing it to be integrated into any LMS
Password awareness game (GAP)	[35]	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	Web-based
Guess Who? - A Serious Game for Cybersecurity Pro-fessionals	[34]	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	Not provided
HATCH	[26]	Proceedings of the 30th International BCS Human Computer Interaction Conference (HCI)	Card game (Non-digital)
The Cyber-RAMPART Training Game	[40]	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial	Not provided

		Intelligence and Lecture Notes in Bioinformatics)	
Persuaded	[24]	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	Online
Phishy	[33]	Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts	Online
PROTECT	[25]	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	Online
Cybersecurity Awareness Game Using Augmented Reality (CybAR)	[41]	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	Mobile Application

RQ1: How has research on the use of SGs to learn about security and privacy been disseminated over time and between countries?

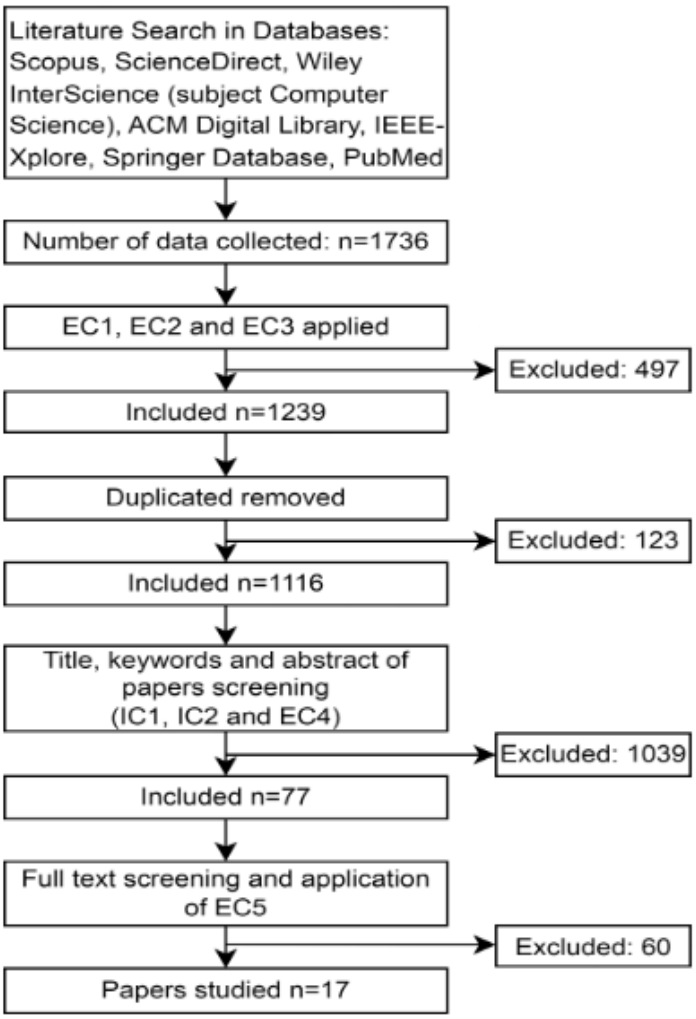

Figure 1. Filtration Method Using particular Criteria.

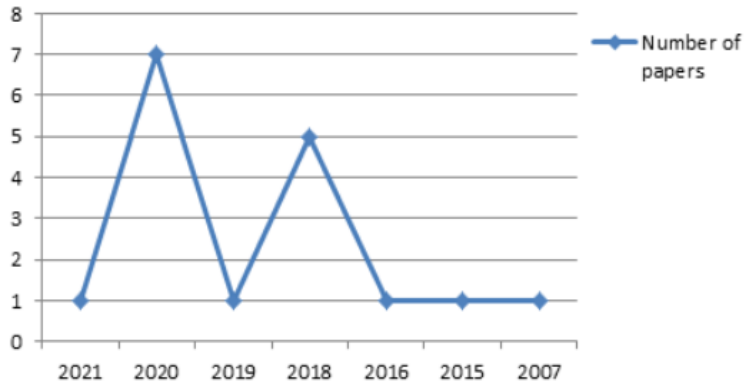

Figure 2. Temporal distribution of the selected papers.

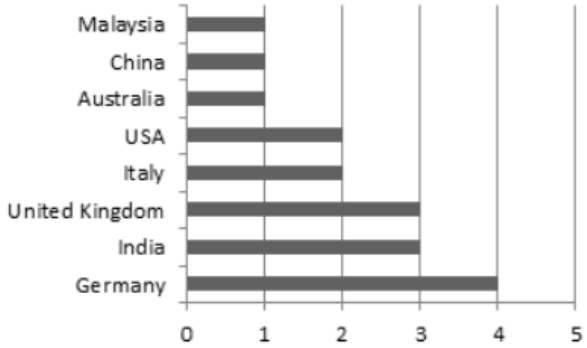

Figure 3. Geographical distribution of the selected papers.

Figure 2 shows the publishing pattern of the papers that were taken into consideration from 2006 to 2021. From 2007 through 2021, all of the chosen studies were published, with 2020 having the highest number of publications (7 articles). The most prolific countries are shown in Figure 3 which was derived from the nationality of the primary author of each of the chosen articles. These graphs show the historical and geographic dispersion of research on the use of SGs to promote security and privacy. The investigation revealed eight nationalities, with Germany being the most active, followed by the United Kingdom and India. However, it seems that interest in the subject is gradually rising on a global scale. Despite conducting research over the course of the last fifteen years, only the recent three years (2018–2020) were the most prolific years in the selected publications. This fact can be a consequence of the COVID-19 pandemic that forced the world to move to online learning, learners, especially in higher education, started to increasingly find traditional learning monotonous, and incapable of holding their attention. Instructors found SGs and web-based educational resources, effective, modern, and appealing [19]. The field of SGs has been rapidly growing and gaining popularity in several fields for more than a decade [7]. The year 2020 will be remembered for more than just the COVID-19 epidemic, the global crisis that changed the world and caused a massive transformation in communication, and work. The year will also be remembered for being the year of cyber-attacks, which increased due to COVID-19 response efforts, as well as the increase in remote work and telemedicine. That year, security specialists have witnessed a significant number of cyberattacks against public and commercial businesses[20]. Almost everyday, phishing tactics, malware assaults, data breaches and ransomware attacks made headlines. Most detrimental, some breaches, such as those using coronavirus-themed phishing attempts and other similar frauds, took longer to

discover and report to specialists. One of the biggest attack happened in March 2020 where Marriott International was a victim of a data breach that compromised the personal information of around 5.2 million clients which caused the leak of contact information, account details for loyalty and additional personal information of hotel guests[21].Two months later, The large healthcare insurance company (Magellan) informed victims of a ransomware assault on May 12. Personal data of both employees and customers have all been successfully hacked. Several Magellan Health companies were included in the attack, and the number of victims was estimated at over 1.7 million. The disaster was due to receiving a phishing email that seemed to be from a Magellan client[22]. In north Europe, another incident took place on October 21, where Finland's leading private psychotherapy practice reported that it was a victim of a data breach in which threat actors obtained personal patient records. The hackers established a new pattern, where they directly blackmailed patients instead of addressing to the organisation and making requests. Even though the government responded immediately to the incident, due to the sensitivity of the information, up until December 2020, Finland police had received 25,000 crime reports[23]. In conclusion, these examples are only a few regarding the numerous cyber threats that happened that year, some of them could have been avoided by taking simple security measures by employees. Unfortunately, human errors play a significant role in triggering these assaults, which proves that an awareness regarding the security and privacy of data to professionals in all kind of fields should be a priority to the organizations. Regarding the geographical distribution of articles discussing SGs as a tool to raise awareness about security and privacy among employees, 50% of the publications in the topic had been written by authors from European nations such as Germany[24][25] [26][27], United Kingdom[28][29][30], and Italy[31][32]. Authors from India [33] [34][35] also contributed with relevant studies. Other countries contributions were less frequent such as USA, Australia and Malaysia that produced one of the most interesting articles about a serious game designed to help healthcare personnel.

RQ2: Which journals are the main targets of articles on SGs to practice data security and privacy?

The chosen articles are disseminated via a variety of publication platforms. Table 3 presents the list of articles along with their references and sources. One study was published in the International Journal of Advanced Computer Science and Applications [36], and another two papers in Computers & Security [29] [37]. The Inter- national Journal of Advanced Computer Science and Applications and Computers Security are both respected journals in their respective fields. However, Computers Security is widely regarded as a prestigious journal within the cybersecurity research community and the premier source of reference for information security research and applications due to its long-standing reputation and significant impact in the field. The journal is directed towards professionals dealing with computer security and data integrity in all sectors[38]. International Journal of SGs published a relevant study [30] that focuses on evaluating the security awareness level of healthcare professionals using an educational game. This journal focuses on manuscripts that provide serious game design for learning purposes and presents innovative solutions to enhance teaching or training scenarios[39]. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) is the most prolific source with nine important publications [28][31] [27][35] [40] [24] [25] [41].

RQ3: What are the environments of SGs?

In this question, we investigated the environments adopted in the selected SGs (Table 3). The most common one was the online and web-based environment with seven games, Persuaded [24], Phishy[33], PROTECT[25], The Cybersecurity Awareness Quiz [27],

CyberCIEGE[37], Password awareness game (GAP)[35], and InfoSecure[36] that the creators made it possible to run on different platforms, browsers, smartphones, and PC. The second most popular environment among the SGs is non-digital and Tabletop, especially card games such as Riskio [29], Cyber Security Requirements Education Game (SREG) [42] and HATCH [26], followed by mobile-based applications like Cybersecurity Awareness Game Using Augmented Reality (CybAR) [41], Role-playing quiz application (RPG) [31]. On the other hand, The SIRET Security Game [32] is playable by exporting it as a SCORM package, allowing it to be integrated into any LMS. The rest of the papers did not provide information regarding this question. In order to produce a successful and engaging experience for the intended audience, it is crucial to recognize that serious game designers' design decisions are impacted by a variety of factors, even though the professional and economical nature of online environments is undoubtedly a major consideration for many game designers. Online settings have clear advantages in terms of cost and professionalism. They offer a user-friendly digital platform that is frequently more affordable than traditional games. Many game creators choose online settings because of their accessibility and affordability. For instance, the inclusion of gamification elements in online environments frequently results in younger players displaying better levels of engagement and drive. Older players, on the other hand, may prefer games with less gamification and a more traditional, physical design. Therefore, it would be oversimplified to state that online environments are only preferred by professional game developers. When choosing design elements for SGs, it is crucial to take into account a variety of other design factors, target audience preferences, and the potential advantages and limitations of both online and physical game environments.

RQ 4. What SGs have pricing and intellectual property?

The games industry depends on intellectual property and relates to intangible properties such as inventions, innovative technology, works of art, and source code. Trademarks, patents, and copyright are all examples of intellectual property. Copyrights, for example, protect the program (code), audio, and graphics in a game. If developers intend to create a new or derivative work based on an existing copyrighted work, they must obtain the necessary licenses from the copyright holders.

Intellectual property for games and software protects the creative and aesthetic components of game development. Intellectual property rights are associated with both the content and the technologies used to make the games. For programmers and other content creators, trademarks, patents, and copyrights are crucial intellectual property protections.

Most of the selected games are still in the early stages of their creation,so at the time of publication of the articles, only a few games were licensed. For example, Riskio[29] is a game created by professors from the University of Southampton, UK, and the work was licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. The game is also available on the official website with a reasonable price (£20.00 plus shipment and payment fees). Phishy[33], on the other hand, is licensed under the ACM publication rights and the author owns the copyright, meaning that digital or hard copies of part of the work or all of it require permission and/or fees if they will be distributed for commercial purposes. In the health sector the game InfoSecure[36] was designed for the Hospital Universiti Kebangsaan Malaysia (HUKM) whereas NHSGGC[30] was directed to staff from The National Health Service Greater Glasgow and Clyde in the United Kingdom. Most of the game's creators received funding from public organizations, ministries, and universities. For instance, CyberCIEGE[37] was mainly supported by the US navy. Organizations of the US Federal Government, schools, and universities were originally expected to use CyberCIEGE free of charge. On the other hand, The Office of Naval Research project Cyber-RAMPART[40] provided funding for the creation of The Cyber-

RAMPART Training Game. The U.S. Government is allowed to reproduce and distribute reprints without regard to any copyright notation.

The European Union, however, supported two relevant research in Germany which is the most prolific country. The CyberSecurity Awareness Quiz[27] received support from the research and innovation program Horizon 2020 of the European Union. Moreover, the online PROTECT game[25] received a grant from the same program. The German Federal Ministry of Education and Research partially supported and granted both the non-digital HATCH game and the online Persuaded game as part of the "IT-Security for Critical Infrastructures" project[26][24]. The Cyber Security Requirements Education Game[42] received funding from both the Natural Science Foundation of China Project and the National Science and Technology Support Program Project. While the government of India supported the "Guess Who?"[34], a game designed for cybersecurity professionals as part of the IMPRINT project.

RQ 5. What are the focus, and scope of SGs?

In the medical field, the InfoSecure[36] serious game was created as a training tool for Hospital Universiti Kebangsaan Malaysia (HUKM) employees to instruct them and enhance their knowledge about information security challenges along with the human responsibilities in maintaining the safety of these critical data. As a result, the serious game produced is confined to information security awareness training for HUKM workers. The paper does not provide a detailed explanation of the scenario used in the developed serious game. However, the paper presents a table that explains how the serious game model elements were implemented in the InfoSecure game. The table contains the components of the serious game model which are game mechanics, factors, design, and storyline. In the medical field, NHSGGC[30] was implemented to measure healthcare staff members' information security awareness. The educational platform simulates healthcare settings, real-world events and crises involving information security, with the intent of making participants conscious of possible security events that could damage health data. Players are tasked with determining the activities that allow medical data to be kept safe by using critical reasoning and formulating realistic solutions to security issues. To generate the educational content of the board game, the authors used as a basis a set of information security regulations that were adopted by The National Health Service Greater Glasgow and Clyde (NHSGGC), to provide players with the knowledge necessary to prevent security issues.

Even though passwords are essential in maintaining the security of personal data, professionals sometimes take this step for granted and do not build a strong password that would make it difficult for hackers to find. In this context, two games were included in our study. On the one hand, a game consisting of a role-playing quiz application [28] focuses on educating common users about passwords and increasing people's awareness of security in general. The game is intended to teach players about issues such as selecting a strong password, avoiding widely used passwords, and practicing proper password hygiene. On the other hand, a web-based game called Password Awareness Game [35] aims at educating users about various insecure password practices. The game scenario is an "escape situation" in which the player controls a tank and navigates through a maze by destroying barriers labeled with weak passwords. The game is designed to be slow-paced and casual, with simple controls and a short gameplay time of less than five minutes.

The developers of the serious game Another Week at the Office[31] focused to assist users and/or security analysts to identify human factor-related threats. The authors had two goals: (1) to create an engaging game that did not require any prior experience to use; (2) to use STRIDE-HF to increase awareness of threats by modeling the potential human factor issues related to cybersecurity breaches that the user might be familiar with. In AWATO, Human Factors have been incorporated by aligning the Human Factors with the STRIDE model which is a threat modeling methodology used to identify and categorize threats to a system.

This means that the STRIDE-HF model which is a theoretical model that considers existing literature on Human Factors within the domain of cybersecurity, is used to focus on errors that are more likely to occur, and how they will occur because of their relevant factor. For instance, employees might skip scanning an uploaded document with anti-virus software or communicate confidential information to unauthorized entities if they are put under stress to save time. The innovative part of this game is the relationship between threat modeling and the Human Factors that have likely caused it.

Another problem that faces employees is how to detect phishing emails. Authors from India designed an online serious game (Phishy) that teaches workers in enterprises about phishing[33]. Their approach teaches employees to recognize short URLs, detect phishing ones using inspection methods, and obtain legal URLs for brand names by searching online. Phishy employs a scenario in which the player assumes the position of Sam, who receives a message on his phone announcing that he has won $5,000 and an all-expense-paid cruise to the Paradise Islands. Sam is then instructed to visit a link to enter bank information and confirm his acceptance of the offer. Without further investigation, he clicks on the link, and it was too late by the time Sam understood it was a phishing message. The robbers had taken all of his money and abandoned him on a boat in the middle of the sea. Through three stages of gameplay, the player has to guide the boat to the land. Another game (Guess Who?)[34], designed to raise phishing awareness, was directed to cybersecurity experts to help them recognize complex phishing emails and threat hunting to find insider malicious activities using a simulated Security Information and Event Management (SIEM) tool. The

SIEM technology is used to detect violations that must be examined by a security analyst. The malicious steps of a threat are encoded in the SIEM tool as violations that are triggered when these activities occur. As a Security Analyst, the player must track down this concealed trail. The game includes adjustable scenarios; therefore, the precise scenario used to play the game may vary based on the requirements of the company at hand. The game contains a training exercise titled ”Insider Threat Hunting on a SIEM Tool” that is separated into three-time segments, with the time restriction scaled and incorporated as the organization’s Security Score. A player is given a list of ten violations in each segment and must examine each offense and connect a certain number of offenses after examining their criteria.

In the context of social engineering, four games have been selected, the card game called Hatch[26] intends to make it possible for regular employees to extract social engineering risks for their workplace with real-life scenarios.

They suggest a serious game that helps players understand how social engineering attackers operate and may be played using a basic office scenario with attackable personalities or a real scenario from the organization or department. Their main purpose is to train people to recognize social engineering attacks in an enjoyable way, which will lead to lasting learning. The scenarios of the game are based on real-life social engineering assaults and may be customized to other sectors and organizations. As an online quiz, the serious game Cybersecurity Awareness Quiz[27] aims to enhance employees’ security awareness, notably against social engineering assaults. The questions are based on real-world social engineering attacks, and the selection of questions is updated on a regular basis with new questions covering current social engineering attacks. This will help employees stay up to date while offering them a fun and engaging experience which distinguishes the CyberSecurity Awareness Quiz from other ways to raise security awareness. Furthermore, the quiz is part of a chain of games aimed at boosting security awareness, which involves playing the aforementioned HATCH. German authors from the Institute of Informatics developed a serious game that uses social psychology defensive mechanisms to teach individuals against social engineering. They also tend to develop persuasive resistance and appeal to a larger population. In 2020 Goeke took the concept of PERSUADED[24] and redeveloped it for the new game called PROTECT[25]. PROTECT is a novel application of PERSUADED’s design

aims and game principles. Both games are intended to prepare employees for social engineering assaults. PROTECT, on the other hand, has greater configuration possibilities, transforming it into a family of games, with PERSUADED being a specific member of the game family. PROTECT's goal is to allow for quick adaption to various scenarios in addition to the player's abilities. Using a different and creative approach the creators of The Cyber-RAMPART Training Game[40] try to increase awareness and develop a "cyber mentality" among users to minimize vulnerabilities and raise attention towards cyber threats. Different from the other games this training tool gives the player the chance to take the profile of an attacker, which the authors believe has several advantages in developing critical thinking and intellectual engagement. In the paper, the player exchanges a conversation with a virtual character and the hacker convinces the player to start an attack by citing different possibilities. The SIRET Security Game[32] is a game aimed at employees from different departments in the public and corporate sectors who are interested in learning how to execute security rules and are not information technology specialists.

They focus on different subjects related to the fundamentals of information security, including fraud prevention, virus protection, and cryptography concepts. Another game designed for non-technology specialists[41], to raise their awareness of the possibility of cybersecurity threats in their regular online activity, comes in the form of an application using augmented reality (Cybersecurity Awareness Game Using Augmented Reality). The scope of the game is to teach people more thoroughly about cybersecurity assaults in a way that is very similar to how they happen.

As aforementioned, some authors decided to use non-digital environments for their SGs. The main objective of the project RISKIO[29] from the University of Southampton in the UK is to provide an educational atmosphere that improves players' knowledge of cybersecurity problems and potential defenses that may be used to prevent or minimize them by highlighting the variety of issues and attack strategies that attackers can employ. In addition, they aim to increase knowledge about the variety of potential measures that may be taken into account to stop, detect, or mitigate cyberattacks while allowing players to practice attacking, finding, and exploiting weaknesses as well as defending against them.

To increase collaboration in the work environment, Yasin et al.[42] designed a multiplayer card game. Cyber Security Requirements Education Game is played with two or more players and is available in two languages to give more players access and a deeper understanding of the scenarios and ideas connected to security. This approach creates a collaborative environment where players work together to defeat competing teams and emphasize team cohesion. The Naval Postgraduate School created the research prototype game CyberCIEGE[37] with scenarios for both IT professionals and public awareness. CyberCIEGE covers a wide variety of cybersecurity subjects, including risk management, network security, access control, cryptography, and incident response, among others, and may be tailored to fit the particular training requirements of various enterprises. The game is unique as it offers an interactive and engaging training experience, as compared to typical training approaches such as formal training sessions or passive computer-based training. The scenarios in the game are meant to be story-driven, with players making resource management decisions that affect an enterprise's productivity and the susceptibility of information assets to virtual attackers. Its interactive and engaging training methodology makes it an effective tool for increasing cybersecurity knowledge and abilities. CyberCIEGE is available to everyone for download. The game is meant to be highly adaptable, which means it can be adjusted to match the particular training requirements of various businesses.

The game's "scenario development language" for constructing new instructional scenarios enables instructors to create custom scenarios that are suited to their organization's particular requirements. For example, the United States Navy used CyberCIEGE to teach both

uniformed and civilian Navy employees. The game may be used to instruct users with varying degrees of technical skill, ranging from novice to advanced.

RQ 6: What game genres are the most/least popular among SGs?

The most popular game genre used by authors in the selected papers is simulation with more than 50% of the games, some of them combined more than one genre and opted for adventure games as well as role-playing, and even the non-digital games contained tabletops that simulated different working environments. Other developers chose to work with the casual genre to reduce players' monotony and offer flexibility and enjoyment.

According to Lameras [15], simulation is a subtype to the learning activity which can be: (1) individual (teacher and student-directed), if it is played by a single player, (2) collaborative (teacher and student-led) if it is a multiplayer game, or (3) discussion and argumentation (reflection), if the teams need to discuss the solution to get to the most accurate one. Game designers choose to simulate a business environment, to reduce the risk and expenses for organisations, and enable players to make errors and learn from them instead of thinking about the effects of their behavior as they would in real life[43]. Games like InfoSecure which simulates a hospital environment or Another Week at the Office, The CyberSecurity Awareness Quiz, and The Cyber-RAMPART Training Game which mimics an office environment, enable the learner to understand, describe, predict, and develop the ability to use the information to solve problems. In addition, this kind of games allow you to analyze and identify patterns or concepts in the data and relate them to previous findings.

Other games that require collaboration or discussion among teammates such as card games Riskio, and Cyber Security Requirements Education Game allow learners to compare ideas, methodologies, or products and make justifiable judgments about their value. The learners may also contribute to society by designing, building, inventing, planning, or producing original knowledge.

One of the least game genres used in the selected papers was adventure games even though it has been proven to teach players to solve problems as well as make decisions or allocate resources because they allow users to learn by doing while also providing visual and auditory stimulation [43]. Phishy[33] was one of the games that used an adventure genre and were created to be visually appealing, and there was also audio output for each action to make the player's journey more enjoyable. The choice of the game genre should not be random. The designers should decide depending on the outcome that they hope to achieve by using this game as a learning tool. Quizzes like role-playing quiz applications also encourage Information transmission which develops a relevant skill which is remembering and memorizing information.

RQ 7: What are the game-related approaches implemented in the SGs?

In the selected articles different game elements and mechanics have been implemented[1]. The most implemented elements that were deployed to motivate the players were rewards and feedback. Notice that more than 60% of the games [33][36] provided the players with motivating messages every time they completed a step.

[1]Game elements, such as points, leaderboards, feedback loops, time constraints, and rewards, originate from the mechanics and dynamics that make traditional games engaging and enjoyable. When these elements are applied to non-game contexts, such as workplaces, learning platforms, or cybersecurity training programs, they are referred to as 'gamification elements.' The term 'gamification' highlights the repurposing of these game elements to motivate user engagement and behavior change in non-game scenarios. However, within serious games, these same components are integrated into a fully structured game environment designed to achieve specific objectives, maintaining their role as 'game elements.

Some authors decided to not use timers, like in the game Phishy, arguing that they could generate an unwelcome feeling of urgency, limiting the game play experience and reducing player satisfaction. They prefer to let the player experiment at his own pace, which results in more engagement. To give them a more realistic experience, players cannot skip decision-making and receive relevant error warnings and learning tips. Six games [36][30][29][27][42][34] used a theme to give the players a more realistic experience while playing the game. On the other hand, the most used game mechanics were role-play and storytelling which increase understanding skills among players. The InfoSecure game used scores at the end of each topic so that users can keep track of their progress. The designers set feedback for the player to receive after answering a question. They also used marks to indicate correct and incorrect responses. Once the player achieves the maximum score in each topic they are offered a certificate as a reward. In addition, they used a hospital theme to help the players feel like they are working in the healthcare sector which might increase learning. Regarding the game mechanics, players can role-play while playing the game which makes it more fun and increases understanding according to Lims' classification based on Bloom's taxonomy[17]. The authors also used scores and the Capture and Eliminate mechanic that develops the ability to adapt information or skills to a new situation.

Unlike InfoSecure, the designers of the National Health Service Greater Glasgow and Clyde game incorporated a game mechanic in which players were given a specific time period to answer questions, increasing the pressure.

In addition, the game was a multiplayer game that promoted collaboration, thus increasing decision-making among players. The game mechanics integrated into both the Role-playing quiz application (RPG) and The CyberSecurity Awareness Quiz included elements such as scoring, competition, and time constraints to enhance engagement and learning.

This game also contained a timer that adds pressure while playing. Moreover, in the case that the player answers incorrectly there will be consequences such as loss of health points. In addition to keeping the players engaged and raising competition, a leaderboard was integrated into the game. The authors used the Question/answers mechanic along with role-playing that increases understanding by providing one or more types of explanations to demonstrate comprehension. Regarding the three card games that were selected, each one used different game elements and mechanics. For instance, in Riskio the player can choose to play as a defender or an attacker, as well as to make it a multi-player game to raise collaboration among players. Along with the aforementioned elements the HATCH game added points as virtual rewards that can be collected. Unlike the previous serious game, Cyber Security Requirements Education Game was time-dependent and offered players badges.

In CybAR you do not only learn about cybersecurity concepts, but you also gain immediate insight into the shocking consequences of cybersecurity attacks produced by careless habits. A total of 20 tasks are included before starting a CybAR game. Other game elements were also included such as scores and levels that help users see and measure their success, while keeping competition by using a leaderboard.

RQ 8: What type of characters are included in the SGS and to what extent do SGs achieve a deep knowledge of the player?

In our study, SG includes imaginary and real characters which we recognize from the work environment. Moreover, Marczewski's classification[44] was considered and we investigated if games take into account player profiles according to the classification that serves as a simple framework for game designers to consider what types of users they may have. Some of the fictional characters were the golden knight that was presented to the user in the Role-playing Quiz to raise password security awareness. The application shows two

characters on the screen, the aforementioned one along with the opponent which is called the dark knight. The user learns about password security in the process as this goes on until one character overcomes the other. In another game (Password Awareness Game) the player must exit a maze to finish the game. In the aforementioned examples, the types of users according to Marczewski's are the user type achiever that is motivated by mastery and wants to learn new things and better themselves this type also desires obstacles to overcome.

In the game InfoSecure the designers replicated a hospital setting to give the player a more realistic game environment. They also allowed the players to choose between pretending to be a nurse, computer hacker, administrative assistant, or ambulance driver. Another game (National Health Service Greater Glasgow and Clyde) contains a game master who serves as an organizer and provides guidance and rules to follow during the game but must refrain from interfering with the participants' decision-making along with a group of three to five participants who will work together as a team to reduce security threats through discussion, but no prior training is necessary. In the game Another Week at the Office, the authors introduced ten different characters, the choice of the characters and their functions within the organization was meant to represent the types of people you would commonly encounter in a workplace. To adapt the gameplay to the player's profile the authors included facilities that are also frequently encountered in the work environment, such as reception, CEO and manager office, general work space, and kitchen. The player and the remaining characters all have work equipment that an employee needs in a workplace, such as a personal computer equipped with all the necessary office programs (e.g. email, word processing, etc.), along with image and document files on their desktop. Similar to the previous game, the card game HATCH contains ten characters HATCH, but the difference is that the player needs to choose whether they belong to the organization as employees or outsiders. The authors presented their positions within the organization, as well as their computer proficiency, and attitudes toward privacy and security. In the previous games the designers opted for the type socializer since they all required collaboration to complete tasks, relatedness motivates this type of player and they seek to communicate with people and form social bonds.

The game CyberCIEGE takes place on board a ship where the player is challenged with completing tasks that improve the organization's security while acting as a security decision-maker. If he fails to do so at the right time the game engine will launch the required attacks and punish the player. This game is intended for achievers since CyberCIEGE proposes challenges to overcome. In the game RAMPAST where the authors introduced a new approach by letting the player assume the role of an attacker by interacting in a chat application with "Hacker Mo," a computer-generated character who persuades the user into carrying out an attack and then walks them through the numerous attack possibilities in a guided discourse. The game is placed in a three-dimensional setting, with other items such as a tablet, a USB key, and a phone that will matter to the player later in the scenario. This game is aimed at Disruptors because the gamer plays the role of troublemaker to disrupt the system.

RQ 9: What evaluation studies have been carried out with those SGs?

As a result of a number of factors, including the expanding technology of Information Technology security and the evolution of attacks [45], it is difficult to conduct a long-term research study to determine the influence of developed SGs on security and privacy awareness. Most of the games focused on evaluating the level of the participants before and after playing the game and collecting feedback regarding their level of satisfaction.

The InfoSecure designers showed the game to computer science professors who have expertise in visual informatics, human computer interaction, and usability to integrate any insightful comments before pilot testing. Then five students from Universiti Kebangsaan Malaysia's faculty of computer science volunteered to participate in the game and to offer

recommendations for improvement. Before making it available to all HUKM personnel, the InfoSecure game underwent an actual pilot test among five employees at the same organization to evaluate its quality and effectiveness. The second round of the pilot test was also attended by the five employees who took part in the first one. The results demonstrated that InfoSecure is a useful tool for the information security awareness training program from both the employees' and the training results' perspectives. The findings also indicate that compared to other areas topics such as privacy and confidentiality, workstation and hacking are more challenging topics for the employees.

During the post-training progress in the employees' performance was observed. The second game directed to health staff NHSGGC was also evaluated by consulting with the IT Compliance Team in the National Health Service Greater Glasgow and Clyde in order to collect feedback on the design. After making the necessary enhancements to comply with the comments of the IT team, four members of the staff participated in the first evaluation phase to ensure that the tests were carried out by medical personnel. Another evaluation round considered three PhD students. The evaluation focused on the performance of the players and to collect feedback on the design and if the game helped them learn more about It security.

Opinions regarding the LEGO-based board design were positive. However, the initial evaluations of the game NHSGGC revealed that participants lacked sufficient understanding of the game's content. Due to the complexity of security controls it is critical that awareness training is delivered in a way that staff members can quickly comprehend. A survey questionnaire was conducted to evaluate the GAP game. After collecting the demographic characteristics of 119 participants the authors conducted a survey to determine the participants' level of awareness regarding password security. They randomly assigned two groups, the first one answered the questions without having any prior training and the second group answered the questions after participating in the game. The group that played the game was also asked to provide feedback regarding the game. The results demonstrated that the experimental group obtained a higher number of correct answers.

The game PERSUADED was evaluated on several occasions during the design stage, by verifying the scenarios and the content of the game. Later on, they performed a case study with 21 university students from different genres and age ranges. The authors collected the technical background of the participants, taking into account their daily use of computers. The participants were asked to answer a pre-questionnaire before watching the game tutorial. For the next phase, the participants played the game and then answered a post-questionnaire that contained the same questions as the first one. The results proved that the participants performed better after playing the game. The game PERSUADED show that social psychology defensive mechanisms may be successfully applied in the area of social engineering. The serious game provides a tool for specifically focusing on risk-taking and decision-making, by introducing new attack scenarios to people and getting their attention in a fun way so they would be interested in learning about social engineering and how to protect oneself from it. A similar evaluation was carried out with the game AWATO, where the participants needed to complete a pre-test questionnaire to determine their level of understanding of threat modeling and cybersecurity themes. Following that, users were invited to complete a Scenario Questionnaire and select three objects after reading through a set of situations in this questionnaire, the first is the error itself, the second is the Human Factor that caused it, and the third is the STRIDE ((Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Escalation of privileges) model element that the fault corresponds to. The third phase asked users to play the game AWATO and identify the same, if not comparable, circumstances that appeared in the scenarios based on the human factor and STRIDE model aspect that they believed was linked with the mistake. Finally, participants were requested to complete a post-study questionnaire identical to the Scenario

Questionnaire. A paired t-test evidenced that playing AWATO improved the understanding of the STRIDE-Human Factors model.

The authors of the card game Riskio performed several studies with staff members and recent graduates to determine the overall effectiveness of raising cybersecurity awareness. The authors analysed the post-task questionnaire's responses to assess three variables: to perceived ease of use (PEU), perceived usefulness (PU) and intention to use (IU) of the Technology Acceptance Model (TAM). Moreover, a unpaired t-test was employed to determine if there were statistical significant differences between students and employees' responses. Participants' perception scores of the Riskio game, for all variables, in increasing awareness in cybersecurity achieved between 3.1 y 4.6 (out of 5). In addition, these scores were higher for employees than for students, with statistical significance in PU and IU ($p<0.05$).

As for the online game PHISHY, a series of evaluations were carried out starting with one week of online availability in a controlled group of 10 contributors, which was eventually extended to a full month due to its enormous success. Participants had to answer a pre-survey before starting the game consisting of identifying phishing URLs by the method of inspection. The same questions were delivered to the player after finishing the game as a post-survey.

Two variables was analyzed: number of licit URLs incorrectly classified as non-legitimate or phishing (FPR) and number of non-legitimate URLs incorrectly classified as licit (FNR). A paired t-test showed a significant statistically decrease in the variables FPR and FNR ($p <0.05$). The results also showed that the online game PHISHY was more beneficial for individuals who knew less about the issue of phishing URLs and emails. Finally, the employees were asked to give their feedback on the game by rating PHISHY on a 5-pt Likert scale, the questions were regarding the fun aspect, education, and if they were able to learn something from the game. Employees found game-based training to be enjoyable and engaging with a 25% of the participants attempted the game more than once.

The card game HATCH also proved its efficiency by allowing 25 full-time workers of the Technical University Munich and Goethe-University Frankfurt to play in the context-specific version of the game and find out if the players could identify potential threats that were peculiar to their settings. The findings imply that players were able to generate threats through gameplay. After that, the authors used the definition of security awareness by Kruger and Kearney which measures the awareness based on behavior, attitude, and knowledge of the employee, to see if playing the game increased participants' knowledge. Therefore, the participants answered a series of questions and rated them on a 5-point Likert scale, to assess security awareness in connection to the assault scenarios in the game. After evaluating the questionnaires, the authors were able to quantify an average improvement in security awareness of between 0.5 and 1 point. Contribution to the State of the Art: While previous studies have demonstrated the potential of SGs in enhancing cybersecurity knowledge, our review brings attention to several gaps in the current literature. In particular, the lack of SGs developed specifically for healthcare professionals is a critical issue given the sensitivity of healthcare data and the potentially severe consequences of security breaches in this field. This study highlights the need for further development and investment in SGs that are tailored to the needs of specialized sectors. Moreover, more empirical research with larger participant groups is essential to establish the long-term effectiveness of SGs as a training tool in cybersecurity education.

In future work, we intend to address this gap by developing a serious game specifically designed to raise the security and privacy awareness of healthcare professionals. This will contribute to the growing field of serious games by offering a solution to the identified shortcomings and ensuring that more sectors can benefit from interactive, engaging, and effective cybersecurity training.

4. Conclusion

This study presents the results of a comprehensive review regarding the use of SGs as tools to teach security and privacy among employees in different sectors. The results of this paper show that SGs can be successfully applied to security and privacy education. SGs are proven to be an enjoyable tool for knowledge acquisition, along with developing abilities and skills such as problem-solving, teamwork, and interested customers in a competitive atmosphere, leading to increased creativity

Although all of the selected games proved to be effective in enhancing information security awareness, most of the games were in a preliminary test phase, which often comprises a smaller sample size and is used to explore the feasibility and viability of the games. More assessments with larger and more varied participant groups would be required to produce more trustworthy and generalizable conclusions. Qualitative studies and case studies focusing on specific contexts and user groups could also provide deeper insights into the practical application and effectiveness of SGs. As a result, a more solid foundation for verifying the selected games could be constructed, and further empirical research is required to thoroughly validate the usefulness of SGs in raising the knowledge level of employees and to test their willingness to use this training tool. Nevertheless, the inclusion of educational components in game design can lead to misunderstandings, inconsistencies, and confusion regarding how learning activities, feedback, and evaluation may be developed and used in games Lameras[15]. Taxonomy and classifications to aid instructional designers, game developers, and academics in more accurately identifying certain learning outcomes using game components are required. The findings of this study reveal a significant shortage of SGs developed especially for professionals employed in specialised sectors, notably healthcare, with only two games identified during the research. In contrast to the growing demand and recognition for SGs in various domains, the availability of such games tailored to meet the specific needs of healthcare professionals remains notably limited. Given the sensitivity of healthcare data, any access by unauthorised users or leak of information can lead to serious and irreversible damages like faulty treatment [46]. Insider attackers can also sometimes compromise protected health information, resulting in data loss, theft, or exposure [47]. These challenges and requirements faced by healthcare professionals and the scarcity of SGs developed to address them indicate a significant gap in the market and emphasizes the need for further attention and investment. In future work, we intend to create a serious game to raise their level of awareness concerning the security and privacy of health data.

Conflicts of interest

All authors declare that they have no conflicts of interest.

References

[1] J. Koivisto, J. Hamari, The rise of motivational information systems: A review of gamification research, International Journal of Information Management 45 (June 2017) (2019) 191–210. doi:10.1016/j.ijinfomgt.2018.10.013.

[2] S. Deterding, D. Dixon, R. Khaled, L. Nacke, From Game Design Elements to Gamefulness: Defining “Gamification”, Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments: ACM. (2011) 9–15
doi:10.1145/2181037.2181040.

[3] W. Hammedi, T. Leclerq, A. C. Van Riel, The use of gamification mechanics to increase employee and user engagement in participative healthcare services, Journal of Service Management.

[4] V. Insley, D. Nunan, Gamification and the online retail experience, International Journal of Retail and Distribution Management 42 (5) (2014) 340–351.
doi:10.1108/IJRDM-01-2013-0030.
[5] M. Pereira, M. Oliveira, A. Vieira, R. M. Lima, L. Paes, The gamification as a tool to increase employee skills through interactives work instructions training, Procedia computer science 138 (2018) 630 -637.
doi:10.1016/j.procs.2018.10.084.
[6] O. Pedreira, F. Garc´ıa, N. Brisaboa, M. Piattini, Gamification in software engineering–a systematic mapping, Information and software technology 57 (2015) 157–168. doi:10.1016/j.infsof.2014.08.007.
[7] F. Laamarti, M. Eid, A. El Saddik, An overview of serious games, International Journal of Computer Games Technology 2014.
doi:10.1155/2014/358152.
[8] D. Michael, S. Chen, Serious games: Games that educate, train, and inform.
[9] L. Sardi, A. Idri, J. L. Fern´andez-Alem´an, A systematic review of gamification in e-health, Journal of biomedical informatics 71 (2017) 31–48.
doi:10.1016/j.jbi.2017.05.011.
[10] S. McKeown, Gamification for Healthcare Improvement: Maximizing motivation and engagement for change (2018) 7–8.
URL https://bcpsqc.ca/wp-content/uploads/2018/03/Gamification-for-Healthcare-Improvement.pdf
[11] International Journal of Serious Games 11 (1) (2024) 83–99.
doi:10.17083/ijsg.v11i1.719, [link].
URL https://journal.seriousgamessociety.org/index.php/IJSG/article/view/719
[12] G. Par´e, M. C. Trudel, M. Jaana, S. Kitsiou, Synthesizing information systems knowledge: A typology of literature reviews, Information and Management 52 (2) (2015) 183–199. doi:10.1016/j.im.2014.08.008.
[13] B. Kitchenham, Procedures for Performing Systematic Reviews, DEBS 2019 - Proceedings of the 13th ACM International Conference on Distributed and Event-Based Systems (2004) 240-243 doi:10.1145/3328905.3332505.
[14] R. W. Wright, R. A. Brand, W. Dunn, K. P. Spindler, How to write a systematic review, Clinical Orthopaedics and Related Research 455 (455) (2007) 23–29.
doi:10.1097/BLO.0b013e31802c9098.
[15] P. Lameras, S. Arnab, I. Dunwell, C. Stewart, S. Clarke, P. Petridis, Essential features of serious games design in higher education: Linking learning attributes to game mechanics, British journal of educational technology 48 (4) (2017) 972–994.
doi:10.1111/bjet.12467.
[16] A. Marczewski, A Revised Gamification Design Framework - Gamified UK - Gamification Expert.
[17] T. Lim, M. B. Carvalho, F. Bellotti, S. Arnab, S. De Freitas, S. Louchart, N. Suttie, R. Berta, A. De Gloria, The lm-gm framework for serious games analysis, Int. J. Serious Games.
[18] L. Sardi, A. Idri, J. L. Fern´andez-Alem´an, A systematic review of gamification in e-Health, Journal of Biomedical Informatics 71 (2017) 31–48.
doi:10.1016/j.jbi.2017.05.011.
[19] T. Anastasiadis, G. Lampropoulos, K. Siakas, Digital game-based learning and serious games in education, International Journal of Advances in Scientific Research and Engineering 4 (12) (2018) 139-144. doi:10.31695/IJASRE.2018.33016.
[20] Pierluigi Paganini, The six biggest cyberattacks of 2020 (2021).
URL https://cybernews.com/security/the-six-biggest-cyberattacks-of-2020/
[21] A. Waldman, 10 of the Biggest Cyber Attacks of 2020 (2021).
URL https://searchsecurity.techtarget.com/news/252494362/10-of-the-biggest-cyber-attacks
[22] L. Toms, Cyber Autopsy Series: Phishing Attack on Magellan Health :: GlobalSign GMO Internet, Inc. (2020).
URL https://www.globalsign.com/en/blog/cyber-autopsy-series-phishing-attack-magellan-health

[23] P. Arntz, Vastaamo psychotherapy data breach sees the most vulnerable victims extorted - Malwarebytes Labs — Malwarebytes Labs (2020).
URL https://blog.malwarebytes.com/cybercrime/2020/10/vastaamo-psychotherapy-data-breach-sees-the-most-vulnerable-victims-extorted/
[24] D. Aladawy, K. Beckers, S. Pape, PERSUADED: Fighting social engineering attacks with a serious game, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 11033 LNCS (2018) 103–118.
doi:10.1007/978-3-319-98385-18.
[25] L. Goeke, A. Quintanar, K. Beckers, S. Pape, PROTECT – An Easy Configurable Serious Game to Train Employees Against Social Engineering Attacks, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 11981 LNCS (2020) 156–171.
doi:10.1007/978-3-030-42051-211.
[26] K. Beckers, S. Pape, V. Fries, HATCH: Hack and trick capricious humans – A serious game on social engineering, Proceedings of the 30th International BCS Human Computer Interaction Conference, HCI 2016 2016-July (2016) 1–3.
doi:10.14236/ewic/HCI2016.94.
[27] S. Pape, L. Goeke, A. Quintanar, K. Beckers, Conceptualization of a cybersecurity awareness quiz, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 12512 LNCS (2020) 61–76.
doi:10.1007/978-3-030-42051-211.
[28] S. Scholefield, L. A. Shepherd, Gamification Techniques for Raising Cyber Security Awareness, in: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 11594 LNCS, Springer Verlag, 2019, pp. 191–203.
doi:10.1007/978-3-030-22351-913.
[29] S. Hart, A. Margheri, F. Paci, V. Sassone, Riskio: A Serious Game for Cyber Security Awareness and Education, Computers and Security 95 (2020) 1–18.
doi:10.1016/j.cose.2020.101827.
[30] M. Pulido, C. W. Johnson, A. Alzahrani, Security awareness level evaluation of healthcare participants through educational games, International Journal of Serious Games 8 (3) (2021) 25–41. doi:10.17083/ijsg.v8i3.459.
[31] L. S. Ferro, F. Sapio, Another week at the office (awato) – an interactive serious game for threat modeling human factors, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 12210 LNCS (2020) 123–142. doi:10.1007/978-3-030-50309-39.
[32] C. D'Apice, C. Grieco, R. Piscopo, L. Liscio, DMS2015short-2: Advanced learning technologies for eLearning in the enterprise: Design of an Educational Adventure Game to teach computer security, Journal of Visual Languages and Computing 31 (2015) 260–266.
doi:10.1016/j.jvlc.2015.10.004.
[33] C. J. Gokul, S. Pandit, S. Vaddepalli, H. Tupsamudre, V. Banahatti, S. Lodha, Phishy - A serious game to train enterprise users on phishing awareness, in: CHI PLAY 2018 - Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended
Abstracts, CHI PLAY '18 Extended Abstracts, Association for Computing Machinery, New York, NY, USA, 2018, pp. 169–181.
[34] S. Gupta, M. P. Gupta, M. Chaturvedi, M. S. Vilkhu, S. Kulshrestha, D. Gaurav, A. Mittal, Guess Who? - A Serious Game for Cybersecurity Professionals, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 12517 LNCS (2020) 421–427.
doi:10.1007/978-3-030-63464-341.
[35] H. Tupsamudre, R. Wasnik, S. Biswas, S. Pandit, S. Vaddepalli, A. Shinde, C. J. Gokul, V. Banahatti, S. Lodha, GAP: A game for improving awareness about passwords, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 11243 LNCS (2018) 66–78.
doi:10.35998/vn-2018-0023.

[36] A. Ghazvini, Z. Shukur, A serious game for healthcare industry: Information security awareness training program for Hospital Universiti Kebangsaan Malaysia, International Journal of Advanced Computer Science and Applications 9 (9) (2018) 236–245.
doi:10.14569/ijacsa.2018.090932.
[37] B. D. Cone, C. E. Irvine, M. F. Thompson, T. D. Nguyen, A video game for cyber security training and awareness, Computers and Security 26 (1) (2007) 63–72.
doi:10.1016/j.cose.2006.10.005.
[38] Computers and Security — Journal — ScienceDirect.com by Elsevier (2021).
URL https://www.sciencedirect.com/journal/computers-and-security
[39] About the Journal — International Journal of Serious Games.
doi:10.17083/ijsg.v11i1.719.
URL https://journal.seriousgamessociety.org/index.php/IJSG/about
[40] R. Wray, L. Massey, J. Medina, A. Bolton, Increasing engagement in a cyber-awareness training game, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 12197 LNAI (2020) 147–158.
doi:10.1007/978-3-030-50439-710.
[41] H. Alqahtani, M. Kavakli-Thorne, M. Alrowaily, The impact of gamification factor in the acceptance of cybersecurity awareness augmented reality game (cybar), Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)
12210 LNCS (2020) 16–31.
doi:10.5465/AMBPP.2020.12210abstract.
[42] A. Yasin, L. Liu, T. Li, J. Wang, D. Zowghi, Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG), Information and Software Technology 95 (2018) 179–200.
doi:10.1016/j.infsof.2017.12.002.
[43] B. Mennecke, D. McNeill, M. Ganis, E. M. Roche, D. A. Bray, B. Konsynski, A. M. Townsend, J. Lester, Second life and other virtual worlds: A roadmap for research (follow-up article to the 2007 international conference on information systems panel), Communications of the Association for Information Systems 18 (28).
doi:10.17705/1CAIS.02220.
[44] A. Marczewski, A Player Type Framework for Gamification Design (2015).
URL http://www.gamified.uk/user-types/
[45] T. E. Gasiba, U. Lechner, M. Pinto-Albuquerque, Cybersecurity challenges in industry: Measuring the challenge solve time to inform future challenges. information 11, 11 (nov. 2020), 533 (2020).
[46] A. H. Seh, M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, R. Kumar, R. A. Khan, Healthcare data breaches: Insights and implications, Healthcare (Switzerland) 8 (2) (2020) 1–18. doi:10.3390/healthcare8020133.
[47] M. Chernyshev, S. Zeadally, Z. Baig, Healthcare Data Breaches: Implications for Digital Forensic Readiness, Journal of Medical Systems 43 (1).
doi:10.1007/s10916-018-1123-2.