Rapid Review

Cybersecurity Awareness Using Gamified Content Training

Alexander Bianca Tofer
albn22@student.bth.se

January 3, 2025

1.0

Table of Contents

1. Introduction

Social engineering attacks in cyber security have emerged as one of the biggest threats to both organizations and private persons worldwide, with attackers increasingly exploiting human psychology rather than using technical vulnerabilities. Despite robust technological safeguards exsisting like firewalls, intrusion detection systems, and encryption protocols, the human element remains the most vulnerable link in the security chain, primarily due to our natural predisposition to trust. As organizations digitize more of their operations and the integration of Internet of Things devices across infrastructure, from healthcare systems to smart city applications and personal home appliances, the attack surface for social engineers continues to expand. Traditional security awareness approaches often fail to engage persons effectively, leading to a growing interest in using gamification as a solution to improve people's awareness of these cyberattacks. A promising method for developing sustainable prevention against social engineering attacks and phishing is serious games. Serious games can be used sensibly and holistically against phishing attacks by increasing IT security awareness [1], [2], [3], [4].

1.1. Structure

The rapid review about cyber security and gamification was conducted in four structured sections: Section 2. Research problem, identify the research problem by critically analyzing existing knowledge and practice in the field. Based on this analysis clear and focused research questions are formulated to act as a guide during the review process.

3. Methodology, developing a search strategy to locate relevant studies through the use of multiple academic databases and then screening the search results against predefined inclusion and exclusion criteria to ensure that only relevant research was considered for the rapid review.

4. Results, extracting data from the selected studies and present a summarizing of the evidence in categorized tables. 5. Conclusion, discuss the potential of threats to validity of the rapid review.

2. Research problem

Conventional methods of delivering security awareness encompass paper and electronic media. Some other methods are formal instructor-led training, video-based, simulation-based and game-based methods. Previous research indicates that conventional cyber security awareness training methods are ineffective [3].

Motivation plays a crucial role in ensuring the sustainable transfer of knowledge. Research shows that knowledge transfer alone often fails to drive a real behavioral change, such as distinguishing phishing from non-phishing emails. Gamification, the application of game design elements in non-game contexts, has emerged as an effective way to address this issue [5].

One specific approach is serious games, which are designed for educational purposes and use interactive, simulated environments to encourage engagement and learning. These games aim to bring about behavioral changes and ensure knowledge retention. By making training enjoyable and interactive, gamification offers a more engaging and impactful learning experience [4].

The research questions (Table 1) have the objectives to identifying the purpose and topics of cyber security awareness games, understanding methods, identifying the audiences, exploring the diffrent game genres, and examining the learning mechanics. Additionally, it provides a critical analysis of the benefits and challenges associated with gamifying cyber security awareness, giving insights for cyber security practitioners.

Table 1: Research questions to be studied in the rapid review.

RQ 1:	How is content gamification implemented in cybersecurity training?
RQ 2:	What empirical evidence demonstrates the effectiveness of gamification in improving cybersecurity awareness and behavior?

3. Methodology

3.1. Search Strategy

To get a manageable number of search results, less than in the search from Figure 1 the focus of the rapid review was limited to specifically on serious games within the field of cyber security. Serious games, which combine education and entertainment, are gaining popularity for their pedagogical benefits and have been used in various fields, including cyber security. These games have proven effective in promoting behavioral change and training, especially in areas like network security, phishing, and end-user protection [3].

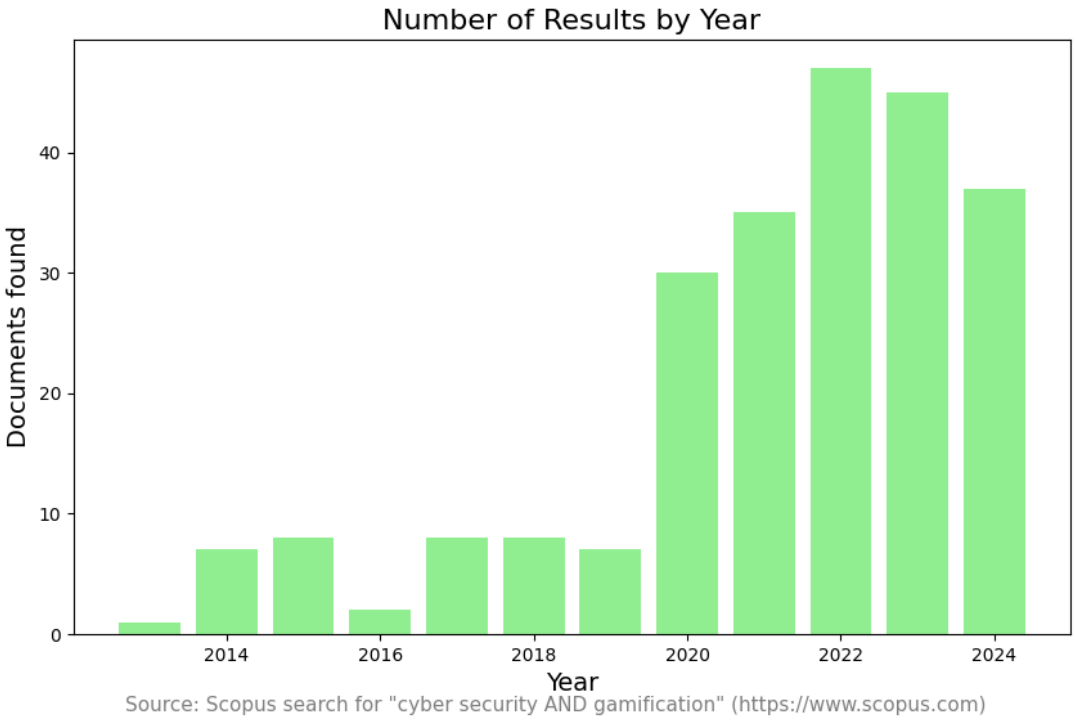

Figure 1: A Scopus search for papers on "cyber security" and "gamification" showed a significant rise in 2020, likely due to the COVID-19 pandemic and the increase in cybersecurity challenges from remote work. Phishing attacks, is estimated to have surged by over 600% during this period [4].

Gamification can be divided into two types: structural gamification and content gamification [5]. Structural gamification primarily involves a template-based approach, which is time and cost-efficient. Examples include points, badges, and leaderboards. On the other hand, content gamification, often referred to as serious games, involves transforming content into a game. This approach requires more time and resources to develop, and once created, it is usually tailored to a specific learning objective. Examples include storytelling, role-playing scenarios, and simulation-based training.

A key factor in selecting the papers with serious games was reusability. If a gamification method can easily adapt to different content and information security topics, it is to be categorized as structural gamification and not a serious game.

Social engineering attacks, particularly phishing[1], were chosen as to be the main topic for the serious games to be include. Due to their significance for both individuals and organizations. Phishing is one of the most common and effective cyber-attacks, exploiting human vulnerabilities to achieve success. This persistent threat shows no signs of slowing down, with attackers frequently targeting user behaviors or online activity to gather information for creating focused and credible attacks [6].

The search terms 'cyber security,' 'serious games,' and 'phishing' were used as the search terms to identify the relevant reserch papers. In order to capture all papers which could be relevant, several synonyms (Table 2) for the search terms were used as well.

Table 2: Synonyms used for the database searches

Search term	**Synonyms used**
cyber security	information security, IT security
serious games	educational game
phishing	social engineering, email fraud

3.3. Search results

The databases Scopus[2], Web of Science[3] and Emerald[4] were searched (Figure 2) using the search terms and synonyms, employing boolean *OR* to include all the synonyms aswell as *AND* to combine the three search terms defined. The publication years were limited to 2020 to 2024 to obtain only the updated and relevant papers, reflecting the fast-evolving nature of cyber security and gamification. No geographic limitations were specified during the search, allowing for the inclusion of papers from all around the world.

Results	Search Database	Search	Years
18	Scopus	("serious game" OR "educational game") AND ("cyber security" OR "information security" OR "IT security") AND ("phishing" OR "social engineering" OR "email fraud")	2020-2024
7	Web of Science	("serious game" OR "educational game") AND ("cyber security" OR "information security" OR "IT security") AND ("phishing" OR "social engineering" OR "email fraud")	2020-2024
26	Emerald	("serious game" OR "educational game") AND ("cyber security" OR "information security" OR "IT security") AND ("phishing" OR "social engineering" OR "email fraud")	2020-2024

Figure 2: The results from searching databases on December 10, 2024, for relevant documents.

1 MITRE ATT&CK framework's description of phishing techniques
2 Scopus
3 Web of Science (WoS)
4 Emerald Publishing

3.2. Inclusion/Exclusion Criteria

The selection process involved applying specific inclusion and exclusion criteria to narrow the scope of the rapid review. Initial screening was conducted by examining each paper's metadata and abstract, which provided sufficient information to evaluate the paper's relevance.

This allowed to only focusing in on cybersecurity awareness training through content gamification with empirical evidence, while excluding any non-english papers, outdated or inaccessible materials, or did not directly address cybersecurity awareness and social engineering attacks.

After applying the criteria outlined in Figure 3: The inclusion and exclusion criteria used for evaluating papers to be included in the rapid review. Seven relevant papers were identified and selected for inclusion in the rapid review.

Inclusion criteria	Exclusion criteria
Only primary empirical studies with quantifiable results	Secondary studies, systematic literature reviews, mapping studies
Research examining a serious game (content gamification)	Papers not about a serious game.
The full text of the paper is available	The full text of the paper is not available
Peer-reviewed research	Gray literature and company reports
The report is written in english.	Studies without any empirical evidence
Research on cybersecurity awareness and including phishing.	Papers not focused on cybersecurity awareness and phishing.
Published in the year 2020 or later	Publications before the year 2020

Figure 3: The inclusion and exclusion criteria used for evaluating papers to be included in the rapid review.

3.3. Data Extraction

The data extraction process involved analyzing the selected papers to identify game topics and research methodologies. This was accomplished through careful review of each study's methodology section, results, and conclusions drawn by the authors. Special attention was paid to the research methods employed and the key findings presented in each paper.

4. Results

4.1. Game genre, topic and focus of serious games

By categorizing the serious game topic and focus (Figure 4) to identify any correlations, it showed that the main focus of four of the games was social engineering, while one focused on mobile usage, one on cyber security, and one on threat modeling. Two games employed the use of frameworks, NIST[5] and STRIDE[6]. Target audience for four of the games was the general public, while three games were specifically designed for IT employees.

Games for the General Public:

(Alma'ariz et al., 2022) *Soceng Warriors* aimed at increasing security awareness against social engineering attacks, particularly phishing, for 14-25-year-old [2].

(Shah & Agarwal, 2023) *Cyber Suraksha* targeted smartphone users, focusing on security awareness and promoting the adoption of security practices for all smartphone users [3].

(Yasin et al., 2024) *PhishDefend Quest* educated users about phishing attacks and the risks of divulging personal information online [1].

(Ihsan et al., 2023) *Datanion* aimed at educating the general public about data privacy and cyber security [7].

IT Professionals:

(Scherb et al., 2023) *Cyberattack Simulation* used both 2D and 3D interactive game play to teach the NIST framework and cyber security concepts for more advanced users [8].

(Ferro et al., 2022) *AWATO* Focused on phishing and categorized human threats using the STRIDE framework [6].

(Kassner & Schönbohm, 2022) *Sir Firewall*[7] an online serious game to increase IT security awareness regarding phishing for IT employees [4].

Study	Serious Game	Genre	Topic	Focus
Alma'ariz et al. (2022)	Soceng Warriors	2D Role playing (RPG)	Social engineering	Increased security awareness against social engineering attacks.
Scherb et al. (2023)	Cyberattack Simulation	3D/2D Interactive	Social engineering	Teaching several cyberattacks using NIST framework for more advanced users.
Yasin et al. (2024)	PhishDefend Quest	Card Game Role playing (RPG)	Social engineering	Improv knolwdge about phishing attacks for general public.
Ihsan et al. (2023)	Datanion	2D Role playing(RPG)	Cyber security	Educate about data security and how to protect their data for general public.
Kassner & Schönbohm (2022)	Sir Firewall	Casual Interactive	Social engineering	Increase IT security awareness for employees.
Ferro et al. (2022)	Another Week a the Office - AWATO	3D Interactive Simulation	Threat Modelling	Identify errors caused by human error and then classify them using STRIDE.
Shah & Agarwal (2023)	Cyber Suraksha	2D Card Game	Mobile apps	Increase threat awareness and motivate to adopt security controls for smartphone users.

Figure 4: Data extraction of the different game types used in the studies.

5 NIST Cybersecurity Framework
6 STRIDE Framework
7 Kassner (Sir Firewall) game in english

4.2. Research method used, data size and findings.

Research methods, data size, and findings were analyzed across the seven studies (Figure 5). All the seven studies choose to use quantitative methods, with five studies (Alma'ariz et al., 2022; Scherb et al., 2023; Yasin et al., 2024; Kassner & Schönbohm, 2022; Ferro et al., 2022) utilizing pre and post surveys to assess security awareness improvements. (Shah & Agarwal, 2023) employed a more unique between-group design with the use of a control group to minimize participation bias. Two of the studies (Yasin et al., 2024; Kassner & Schönbohm, 2022) supplemented their quantitative data with qualitative data insights through post interviews performed.

Regarding demographics, three studies used student participants: (Alma'ariz et al., 2022) targeted students aged 14-25, (Yasin et al., 2024) used university students, and (Shah & Agarwal, 2023) focused on college students. Two studies (Scherb et al., 2023; Kassner & Schönbohm, 2022) were conducted with IT employees. (Ihsan et al., 2023) and (Ferro et al., 2022) did not specify their participant demographics.

Sample sizes varied considerably, ranging from 10 to 97 participants. The largest sample was (Yasin et al., 2024) with 97 participants, while (Ihsan et al., 2023) had the smallest with only 10 samples.

All studies reported positive outcomes in improving security awareness. The most positiv was, (Alma'ariz et al., 2022) that concluded "*Results prove that this game can be used to increase security awareness of social engineering attacks*," while (Shah & Agarwal, 2023) found participants in the intervention group were 2.65 times more likely to adopt recommended security behaviors.

Study	Research Method	Control group	Data Size	Demographical	Findings
Alma'ariz et al. (2022)	Quantitative data from pre and post surveys		30	Students 14 to 25 years	*"Results prove that this game can be used to increase security awareness of social engineering attacks"*
Scherb et al. (2023)	Quantitative data from pre and post surveys		32	IT employees	*"Has a positive short term effect on increasing cybersecurity awareness"*
Yasin et al. (2024)	Quantitative data from surveys, and qualitative observations		97	Students	*"Game successfully improved players' comprehension of phishing threats and how to detect them."*
Ihsan et al. (2023)	Quantitative data from survey		10		*"Effectively teaches cybersecurity concepts, though there is room for improvement in user engagement and content "*
Kassner & Schönbohm (2022)	Quantitative data from surveys and qualitative interviews		61	IT employees	*"A subjective increase in IT security awareness."*
Ferro et al. (2022)	Quantitative data from pre and post surveys		19		*"Has shown the capacity to educate users while also offering a tool to aid users in comprehending the threat modelling process."*
Shah & Agarwal (2023)	Quantitative data from between-group.	Yes	94	Students	*"The results indicate that the participants in the intervention group are 2.65 times more likely to adopt recommended behaviour."*

Figure 5: Data about the research method and findings were extracted from all seven studies.

5. Conclusion

5.1. Threats to validity

The generalizability is limited due to small sample sizes used in all the studies examined, with all studies having fewer than 100 samples, and also a narrow participant selection that may not represent the broader population. (Shah & Agarwal, 2023) acknowledged that their sample was restricted to students, limiting the findings applicability to the broader smartphone user population.

A significant limitation across studies was the lack of long-term effectiveness evaluation. (Scherb et al., 2023) pointed out this limitation, noting "*Our study only analyzed the short term effects, as we did not perform any assessment a longer period after playing the game (e.g., half a year or a year later).*" This raises questions about the durability of learning outcomes and whether the security awareness improvements persist over time. The absence of any long-term studies makes it difficult to determine if these games create lasting behavioral changes in cyber security practices. (Ferro et al., 2022) highlighted the lack of extensive empirical testing, also raising concerns about long-term educational efficacy. They also noted that some widely recommended best practices in the field lack robust empirical support, potentially affecting the validity of conclusions.

5.2. Discussion and reflections

The findings from the rapid review highlight the potential of using serious games to enhance cyber security awareness, in areas like social engineering attacks. One significant drawback to why adoption rate still might be low could be the cost of implementing structured gamification, either through developing or purchasing a serious game. No study provided any estimates of the cost to implement a serious game.

Organizations would need to weigh the cost of developing or purchasing such tools against the potential benefits, including increased employee engagement and reduced cyber security risk for the company. It's important to consider whether the return on investment justifies the initial costs, especially when other training methods may be available at a lower price point.

Non of the studies did presented any alternative methods to achieve the same or similar goal as a serious game, such as traditional training programs, workshops, or simulations, which could offer different advantages, particularly for organizations that may have budgetary or resource constraints.

While gamification has shown promise in improving cybersecurity awareness, future studies should explore how this approach compares with more traditional training techniques. Additionally, research could investigate long-term efficacy of gamified learning tools versus other forms of cyber security training.

6. References

Bibliography

[1] Yasin, A., Fatima, R., JiangBin, Z., & Afzal, W., Can serious gaming tactics bolster spear-phishing and phishing resilience?: Securing the human hacking in Information Security. (2024), Information and Software Technology, 170, Article 107426. URL https://www.diva-portal.org/smash/get/diva2:1858325/FULLTEXT01.pdf

[2] Alma'ariz, S., Girinoto, Hadiprakoso, R. B., & Qomariasih, N., Soceng Warriors: Game-based learning to increase security awareness against social engineering attacks. (2022), 2022 IEEE 8th Information Technology International Seminar (ITIS), 58–63. URL https://ieeexplore.ieee.org/document/10009041

[3] Shah, P., & Agarwal, A., Cyber Suraksha: A card game for smartphone security awareness. (2023), Information & Computer Security, 31(5), 576–600. URL https://www.emerald.com/insight/content/doi/10.1108/ics-05-2022-0087/full/html?skipTracking=true

[4] Kassner, L., & Schönbohm, A., A serious game to improve phishing awareness. (2022), In K. Kiili et al. (Eds.), GALA 2022, Lecture Notes in Computer Science (Vol. 13647, pp. 109–117). Springer. URL https://doi.org/10.1007/978-3-031-22124-8_11

[5] Bitrián, P., Buil, I., Catalán, S., & Merli, D., Gamification in workforce training: Improving employees' self-efficacy and information security and data protection behaviours. (2024), Journal of Business Research, 114685. URL https://doi.org/10.1016/j.jbusres.2024.114685

[6] Ferro, L. S., Marrella, A., Catarci, T., Sapio, F., Parenti, A., & De Santis, M., AWATO: A serious game to improve cybersecurity awareness. (2022), In X. Fang (Ed.), HCII 2022, Lecture Notes in Computer Science (Vol. 13334, pp. 508–529). Springer. URL https://link.springer.com/chapter/10.1007/978-3-031-05637-6_33

[7] Ihsan, S. N., Abd Kadir, T. A., Ismail, N. I., Yuan, K. Z., & Song Jie, Y., Implementation of serious games for data privacy and protection awareness in cybersecurity. (2023), Proceedings of the 2023 IEEE 8th International Conference on Software Engineering and Computer Systems (ICSECS), 330-336. URL https://doi.org/10.1109/ICSECS58457.2023.10256329

[8] Scherb, C., Heitz, L. B., Grimberg, F., Grieder, H., & Maurer, M., A cyberattack simulation for teaching cybersecurity (2023), In A. Gerber & K. Hinkelmann (Eds.), Society 5.0 2023 (EPiC Series in Computing, Vol. 93) (pp. 129–140). URL https://easychair.org/publications/open/T5tcp