ANALYSIS OF GAMIFICATION IN CYBERSECURITY EDUCATION FOR STUDENTS: A SYSTEMATIC LITERATURE REVIEW

Reisa Aulia Sodikin[1]
Universitas Pendidikan Indonesia, Indonesia
E-mail : reisaaulias@upi.edu

Rizki Hikmawan[2]
Universitas Pendidikan Indonesia, Indonesia
E-mail : hikmariz@upi.edu

DOI : http://dx.doi.org/10.30983/educative.v8i2.7513

Submission: October 15, 2023	*Revised: December 16, 2023*	*Accepted : December 22, 2023*	*Published: December 29, 2023*

Abstract

The increasingly complex digital era requires a deeper comprehension of cybersecurity threats, particularly in educational settings. The imperative to establish an interactive and adaptive learning environment, responsive to technological advancements, makes the adoption of gamification elements as an innovative method to heighten student involvement and deliver crucial knowledge in the context of cybersecurity. To tackle these challenges, this research outlines the cause-and-effect relationships, focusing on the connection between the evolution of cybersecurity knowledge areas and gamification elements found in earlier literature. By specifying the components of the CIA Triad—Confidentiality, Integrity, and Availability—this study establishes a strong foundation for investigating how gamification elements can harmonize with the cybersecurity requirements in this digital era. The research utilizes a systematic literature review method based on inclusion and exclusion criteria, the research identifies 13 Google Scholar-indexed articles published between 2018 and 2023. These findings reveal a correlation between gamification elements and the CIA Triad aspects, along with Venn diagrams in recent cyber threats and attacks. This offers a foundation for the development of more potent pedagogical approaches in delivering cybersecurity materials to the generation maturing in this digital era.

Keywords: CIA Triad, Gamification, Cybersecurity, Cybersecurity Education, Systematic Literature Review

Abstrak

Era digital yang semakin kompleks menuntut pemahaman yang lebih mendalam terhadap ancaman keamanan siber, khususnya di lingkungan pendidikan. Adapun kebutuhan untuk menciptakan lingkungan pembelajaran yang menarik dan responsif terhadap perkembangan teknologi informasi mendorong penerapan elemen-elemen gamifikasi sebagai metode inovatif yang dapat meningkatkan keterlibatan siswa dan menyampaikan pengetahuan krusial dalam konteks keamanan siber. Dalam rangka mengatasi tantangan ini, penelitian ini menjelaskan secara rinci pola sebab dan akibat, dengan fokus pada korelasi antara pengembangan area wawasan keamanan siber dengan elemen-elemen gamifikasi dalam literatur terdahulu. Dengan merinci aspek-aspek CIA Triad, yakni Confidentiality, Integrity, dan Availability, penelitian ini menciptakan dasar yang kuat untuk mengeksplorasi bagaimana elemen-elemen gamifikasi dapat menyelaraskan diri dengan kebutuhan keamanan siber di era digital ini. Penelitian ini menggunakan metode systematic literature review berdasarkan kriteria inklusi dan eksklusi, menghasilkan 13 artikel terindeks Google Scholar yang diterbitkan di tahun 2018-2023. Hasil penelitian menunjukkan adanya korelasi antara elemen-elemen gamifikasi dan aspek CIA Triad, serta diagram venn yang mengilustrasikan kesesuaian elemen gamifikasi dengan aspek CIA Triad pada ancaman dan serangan siber terbaru sehingga dapat memberikan landasan untuk pengembangan pedagogi yang lebih efektif dalam menyampaikan materi keamanan siber kepada generasi yang tumbuh dalam era digital ini.

Kata Kunci: *CIA Triad, Gamifikasi, Keamanan siber, Pendidikan Keamanan siber, Tinjauan literatur sistematis*

Introduction

In the realm of education, enjoyable learning experiences can boost children's motivation to actively participate in their studies. A teaching approach that has gained significant attention in recent years is known as gamification. This term was established by Nick Pelling in 2002, gamification gained widespread recognition and acceptance around 2010[1]. Essentially, gamification involves applying principles from games to non-

[1] Antonia Ypsilanti and others, 'Are Serious Video Games Something More than a Game? A Review on the Effectiveness of Serious Games to Facilitate Intergenerational Learning', *Education and Information Technologies*, 19.3 (2014), 515–29 <https://doi.org/10.1007/s10639-014-9325-9>.

game contexts[2,3]. The primary aim is to enhance student engagement by creating stronger experiences in everyday situations through game-like mechanisms[4]. With gamification in education, students gain the ability to control their actions, learn from mistakes and experimentation, and acquire a wealth of knowledge, experience, and skills in a short period. Gamification has progressively been recognized as an effective teaching method to enhance student comprehension and create an engaging learning environment[5]. Many researchers have proven that gamification is not only effective in subject-focused classroom learning but also in acquiring crucial knowledge and skills needed in current life situations[6].

Katja and Ellen's research proves that gamification effectively enhances students' comprehension, specifically in the realm of science education. They conducted a study with third-year MedLab Science students, demonstrating an improved understanding of Enzyme-Linked Immunosorbent Assays (ELISAs) through a web-based digital laboratory[7]. Similarly, Maria and Cristina's study affirms the effectiveness of gamification in increasing student engagement, fostering positive ecological thinking, and developing digital literacy skills in elementary school students. This was evident in their program aimed at boosting ecological awareness and digital literacy among elementary students in the northwest region of Spain[8].

One crucial and increasingly urgent area of knowledge to acquire in today's digital era is understanding cybersecurity. This field is closely associated with the internet and the virtual realm. The internet serves as a global network enabling interactive communication without constraints of space and time[9]. Its presence has implications for diverse aspects of life, including business, education, and social interactions[10]. More than just a tool for meeting informational needs, the Internet is an effective medium for human communication in the virtual world. The virtual world is a parallel universe shaped and upheld by the computer realm, fostering global knowledge exchange, information sharing, and entertainment[11,12]. Ideally, the internet should be a secure and comfortable space for accessing information, communication, and relationship-building. Unfortunately, in reality, the internet is often a target for cyberattacks that pose risks to both individuals and organizations.

Furthermore, in today's digital era, children spend numerous hours exploring the internet

[2] Karen Robson and others, 'Is It All a Game? Understanding the Principles of Gamification', *Business Horizons*, 58.4 (2015), 411–20 <https://doi.org/10.1016/j.bushor.2015.03.006>.

[3] Kevin Werbach and Dan Hunter, 'For the Win: How Game Thinking Can Revolutionize Your Business: 9781613630235: Amazon.Com: Books', *Universadad de Pensylvania*, 2012, 146 <https://www.amazon.com/Win-Game-Thinking-Revolutionize-Business/dp/1613630239/ref=pd_sim_14_3?_encoding=UTF8&psc=1&refRID=4FRM3MYBDM74G24R5R8Q>.

[4] Jung Tae Kim and Won Hyung Lee, 'Dynamical Model for Gamification of Learning (DMGL)', *Multimedia Tools and Applications*, 74.19 (2015), 8483–93 <https://doi.org/10.1007/s11042-013-1612-8>.

[5] Zamzami Zainuddin and others, 'The Role of Gamified E-Quizzes on Student Learning and Engagement: An Interactive Gamification Solution for a Formative Assessment System', *Computers and Education*, 145 (2020), 103729 <https://doi.org/10.1016/j.compedu.2019.103729>.

[6] Crystal Callista Anak Yunus and Tan Kim Hua, 'Exploring a Gamified Learning Tool in the ESL Classroom: The Case of Quizizz', *Journal of Education and E-Learning Research*, 8.1 (2021), 103–8 <https://doi.org/10.20448/JOURNAL.509.2021.81.103.108>.

[7] Katja Fleischman and Ellen Ariel, 'Gamification in Science Education: Gamifying Learning of Microscopic Processes in the Laboratory', *Contemporary Educational Technology*, 7.2 (2020), 138–59 <https://doi.org/10.30935/cedtech/6168>.

[8] María Carmen Ricoy and Cristina Sánchez-Martínez, 'Raising Ecological Awareness and Digital Literacy in Primary School Children through Gamification', *International Journal of Environmental Research and Public Health*, 19.3 (2022) <https://doi.org/10.3390/ijerph19031149>.

[9] Qing Wang and others, *Intelligent Crowdsourced Testing*, *Intelligent Crowdsourced Testing*, 2022 <https://doi.org/10.1007/978-981-16-9643-5>.

[10] Andrew Keen, *The Internet Is Not the Answer* (Atlantic Books Ltd, 2015).

[11] Michael Benedikt, 'Introduction to Cyberspace: First Steps', *Cyberspace: First Steps*, 1991, 458 <https://archive.org/details/CyberspaceFirstSteps/mode/2up>.

[12] David Bell, *An Introduction to Cybercultures* (Routledge, 2006).

daily. In the online world, they encounter various potential risks associated with cybercrimes. However, lacking adequate understanding, they are unable to assess these cyber threats, and unknowingly, they expose themselves to the dangers of cybercrimes, such as unintentionally revealing personal information. Children are also vulnerable to falling victim to cybersecurity threats like social manipulation, cyberbullying, hacking, virus and malware attacks, as well as cyberstalking through search engines, advertisements, and social media platforms like Facebook, Twitter, and various other websites[13].

Cybersecurity threats are heavily dependent on the public's understanding of these threats, their ability to assess risks, and their capability to apply knowledge to mitigate these risks[14]. Hence, there is a need to reduce the risks of cybersecurity threats caused by human actions by enhancing users' comprehension of cybersecurity and privacy issues. Cybersecurity education is especially vital and crucial, especially among students who are consistently digitally connected, given the integral role of information technology in the educational setting. Cybersecurity is closely linked to safeguarding data and information stored, processed, and transmitted within the digital environment.

Information system security consists of safeguarding the following aspects:

(1) Confidentiality, this aspect ensures the secrecy of data or information, ensuring that only authorized individuals can access the information and ensuring the confidentiality of data in transit, at rest, and in storage;

(2) Integrity, integrity ensures that data cannot be altered without the permission of authorized parties. It maintains the accuracy and completeness of information and its processing methods to ensure integrity;

(3) Availability, availability ensures that data is accessible when needed, guaranteeing that authorized users can utilize information and associated devices (relevant assets when required)[15].

These three parameters are known as the CIA (Confidentiality, Integrity, and Availability) or CIA Triad.

Figure 1. CIA Triad[16]

CIA serves as the central and fundamental principle of the ISO 27001 information security standard. ISO 27001:2013 is a certification standard released by the International Organization for Standardization (ISO). It deals with the Information Security Management System (ISMS), providing general guidance on the actions organizations or companies need to take when implementing information security concepts. Regardless of the scale or extent of the target, whether within an organization or for individuals, the CIA encompasses the aspects of information security susceptible to cyber threats and attacks.

[13] Zainab Hamdan and others, 'Protecting Teenagers from Potential Internet Security Threats', *Proceedings of the 2013 International Conference on Current Trends in Information Technology, CTIT 2013*, 2013, 143–52 <https://doi.org/10.1109/CTIT.2013.6749493>.

[14] Eyvind Garder B. Gjertsen and others, 'Gamification of Information Security Awareness and Training', *ICISSP 2017 - Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, 2017-Janua.January (2017), 59–70 <https://doi.org/10.5220/0006128500590070>.

[15] Irsyat Iffano Riyanarto Sarno, *Sistem Manajemen Keamanan Informasi* (Surabaya: ITS Press, 2009).

[16] Jussi Nikander, Onni Manninen, and Mikko Laajalahti, 'Requirements for Cybersecurity in Agricultural Communication Networks', *Computers and Electronics in Agriculture*, 179.September (2020), 105776 <https://doi.org/10.1016/j.compag.2020.105776>.

Although they may seem similar, cybersecurity threats and cyberattacks have different meanings. Abu defines cybersecurity threats as situations where there is a possibility of malicious activities, while a cyberattack occurs when these incidents happen[17]. Idrajit suggests that an event qualifies as a cyberattack if the criminal successfully exploits vulnerabilities in technology systems, leading to the occurrence of the feared threats[18]. In simpler terms, cybersecurity threats represent potential dangers, while cyberattacks are the actual occurrence of those potential dangers.

Attacks are categorized into three types:

(1) Passive attack; occurs when an intruder stops ongoing data through the network without taking any other active measures;
(2) Active attack; involves the intruder gaining access to disrupt the network's operating system employing more aggressive actions to interfere with network operations;
(3) Advanced attack; involves sophisticated intrusion processes, becoming more intricate and incorporating a series of continuous actions against the intrusion process[19].

Meanwhile, threats are divided into two categories:

(1) Active threats; include data theft, unauthorized system usage, illegal data destruction, and unauthorized modifications;
(2) Passive threats; include system failures, human errors, and natural disasters[20].

In providing cybersecurity education to students, Robson, within the context of cybersecurity science, suggests that providing theoretical content is considered less effective as students may struggle to understand it practically, particularly when facing actual cyber threats[21]. Furthermore, based on Werbach's research, individuals tend to learn only 20% of what they hear and read, but they can absorb 90% of what they actively practice[22].

Hence, there is a need for further investigation into the utilization of gamification in cybersecurity education, drawing insights from previous studies. The objective of this study is to establish a connection between cybersecurity knowledge areas and gamification elements identified in prior literature. The aim is to pinpoint gamification elements aligned with the CIA Triad aspects for implementation in cybersecurity education for students, addressing both current and anticipated future cybersecurity threats and attacks. This research serves as a comprehensive exploration, laying a strong foundation for enhancing the effectiveness of cybersecurity education amidst the evolving landscape of cybersecurity threats and attacks.

To review recent literature on gamification in cybersecurity education for students, the following questions are utilized:

1. How do cybersecurity knowledge areas correlate with the gaming elements applied in previous literature?
2. Which gamification elements are appropriate for implementing in cybersecurity education for students, particularly addressing recent or anticipated future cybersecurity threats and attacks based on the CIA Triad?

[17] Md Sahrom Abu and others, 'Cyber Threat Intelligence – Issue and Challenges', *Indonesian Journal of Electrical Engineering and Computer Science*, 10.1 (2018), 371–79 <https://doi.org/10.11591/ijeecs.v10.i1.pp371-379>.

[18] R E Indrajit, 'Enam Aspek Menjaga Dan Melindungi Dunia Maya', … *(Internet and Infrastructure/Coordination Center)* …, 2017 <https://www.academia.edu/download/33264299/Aspek_menjaga_dan_melindungi_dunia_maya.pdf>.

[19] Mohan V. Pawar and J. Anuradha, 'Network Security and Types of Attacks in Network', *Procedia Computer Science*, 48.C (2015), 503–6 <https://doi.org/10.1016/j.procs.2015.04.126>.

[20] Paryati, 'Keamanan Sistem Informasi', *Seminar Nasional Informatika 2008 (SemnasIF 2008) UPN 'Veteran' Yogyakarta, 24 Mei 2008*, 2008.semnasIF (2008), 379–86.

[21] Robson and others.

[22] Werbach and Hunter.

Research Method

The systematic literature review is the chosen method to collect, assess, and analyze all relevant literature on the investigated topic[23]. The benefits of employing systematic literature review for researchers include offering comprehensive evidence for decision-making. In this study, the systematic literature review method is applied to investigate prior research on the utilization of gamification methods in cybersecurity education for students.

This review guideline focuses on aspects such as formulating research questions, establishing criteria for the inclusion and exclusion of articles, and selecting reliable databases to ensure the accuracy and credibility of the data. The data for this study is sourced from the Publish or Perish database. The inclusion and exclusion criteria for the reviewed articles include: (1) Excluding literature review articles; (2) Publications within the last 5 years, specifically from 2018 to 2023; (3) Studies addressing topics related to cybersecurity and gamification; (4) Article content aimed at improving users' understanding and knowledge of cybersecurity.

The information gathering process commenced by initially identifying 992 articles meeting the search criteria with keywords such as Gamif*, "Cyber security", and Cybersec. From this total, a selection was made with a focus on reputable international publishers, including Elsevier, IEEE Xplore, Springer, Taylor & Francis, Wiley Online Library, ProQuest, Emerald, ERIC, and Sage Journals, resulting in 408 relevant articles. These articles were then further refined based on the established inclusion and exclusion criteria, leading to a final selection of 13 articles indexed in Google Scholar. Therefore, 13 articles will undergo comprehensive analysis in this research.

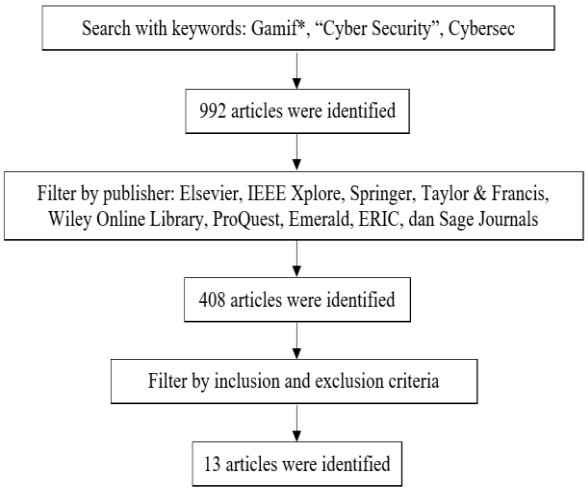

Figure 2. Research methodology flow in this systematic literature review

Finding and Discussion

Finding

Analysis of knowledge areas and gamification elements in cybersecurity education in the literature

In this systematic literature review, the Publish or Perish database was employed to chart literature publications implementing gamification in cybersecurity education. The objective was to pinpoint the utilization of gamification in the education of cybersecurity for students. Through an examination of relevant previous studies, this research delivers a clear and comprehensive overview of how gamification is employed in cybersecurity education within the educational framework. Table 1 presented below provides an overview analysis of the use of gamification in cybersecurity education.

[23] Yudin Wahyudin and Dhian Nur Rahayu, 'Analisis Metode Pengembangan Sistem Informasi Berbasis Website: A Literatur Review', *Jurnal Interkom: Jurnal Publikasi Ilmiah Bidang Teknologi Informasi Dan Komunikasi*, 15.3 (2020), 26–40 <https://doi.org/10.35969/interkom.v15i3.74>.

Table 1. Overview analysis of the use of gamification in cybersecurity education

Author	Year	Source type	Knowledge area	Gamification element
Scholefield, S. & Shepherd, L. A.[24]	2019	Conference paper	Strong password	Time interval, points, leaderboard
DeCarlo, S. M.[25]	2020	Dissertation	Sensitive data security	Goals, rules, competition, time interval, badges, points, leaderboard, levels
Abu-Amara, F., et al.[26]	2021	Journal	Strong passwords, phishing, physical security	Levels
Qusa, H. & Tarazi, J.[27]	2021	Conference paper	Strong passwords	Levels, time interval
Diakoumakos, J., et al.[28]	2021	Conference paper	Online privacy	Points, levels, task, hint, time interval
Kvietinskaitė, G., et al.[29]	2022	Conference paper	Online privacy	Levels, points
Faith, B. F., et al.[30]	2022	Conference paper	Clickjacking	Points
Matovu, R., et al.[31]	2022	Conference paper	Social engineering, phishing, spear-phishing, vishing, smishing, baiting, tailgating, malware, virus, cyberbullying, cyberstalking, identity theft, and worms	Leaderboard, reward, time interval
Brady, C. & M'manga, A.[32]	2022	Conference paper	Social engineering, denial of service, strong passwords	Levels, card, matching, memory
Broholm, R., et al.[33]	2022	Conference paper	Online privacy	Achievements, task, points, Streaks, challenges, nudging
McClaskey, T. M.[34]	2022	Capstone Project	Phishing	Challenges, goals
Alothman, B., et al.[35]	2023	Preliminary studies	Strong passwords, phishing, hijacking	Reward, roles
McLaughlin, K.[36]	2023	Dissertation	Online privacy	Leaderboard, achievement, badges

[24] Sam Schole and Lynsay A Shepherd, 'Gami Fi Cation Techniques for Raising Cyber Security Awareness', 2019, 191–203 <https://doi.org/10.1007/978-3-030-22351-9>.

[25] Sean M DeCarlo, 'Measuring the Application of Knowledge Gained from the Gamification of Cybersecurity Training in Healthcare', May, 2020, 90

[26] Abu and others.

[27] Hani Qusa and Jumana Tarazi, 'Cyber-Hero: A Gamification Framework for Cyber Security Awareness for High Schools Students', *2021 IEEE 11th Annual Computing and Communication Workshop and Conference, CCWC 2021*, 2021, 677–82 <https://doi.org/10.1109/CCWC51732.2021.9375847>.

[28] Jason Diakoumakos and others, 'Cyber-Range Federation and Cyber-Security Games: A Gamification Scoring Model', *Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience, CSR 2021*, 2021, 186–91 <https://doi.org/10.1109/CSR51186.2021.9527972>.

[29] and Virgilijus Krinickij Gabriel˙e Kvietinskait˙e, Linas Bukauskas, 'Cyber Security Table-Top Exercise Gamification with Dynamic Scenario for Qualification Assessment', *Springer*, 1654 (2022), 54–62 <https://doi.org/https://doi.org/10.1007/978-3-031-19679-9_8>.

[30] B. Fatokun Faith and others, 'An Intelligent Gamification Tool to Boost Young Kids Cybersecurity Knowledge on FB Messenger', *Proceedings of the 2022 16th International Conference on Ubiquitous Information Management and Communication, IMCOM 2022*, 2022 <https://doi.org/10.1109/IMCOM53663.2022.9721733>.

[31] Richard Matovu and others, 'Teaching and Learning Cybersecurity Awareness with Gamification in Smaller Universities and Colleges', *Proceedings - Frontiers in Education Conference, FIE*, 2022-Octob (2022), 1–9 <https://doi.org/10.1109/FIE56618.2022.9962519>.

[32] Callum Brady and Andrew M'Manga, 'Gamification of Cyber Security Training-EnsureSecure', *Proceedings - 2022 IEEE International Conference on e-Business Engineering, ICEBE 2022*, 2022, 7–12 <https://doi.org/10.1109/ICEBE55470.2022.00010>.

[33] Rasmus Broholm, Michael Christensen, and Lene Tolstrup Sorensen, 'Exploring Gamification Elements to Enhance User Motivation in a Cyber Security Learning Platform Through Focus Group Interviews', *Proceedings - 7th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2022*, 2022, 470–76 <https://doi.org/10.1109/EuroSPW55150.2022.00056>.

[34] Tiffany M. McClaskey, 'Tabletop Exercises: Gamification in Cybersecurity', *ProQuest* (Utica University, 2022).

[35] Basil Alothman and others, 'Towards Enhancing Cyber Security Awareness Using Gamification Escape Room', *International Conference on Ubiquitous and Future Networks, ICUFN*, 2023-July (2023), 828–30 <https://doi.org/10.1109/ICUFN57995.2023.10199673>.

[36] Kevin Mclaughlin, 'A Quantitative Study of Learner Choice in Cybersecurity Training: Do They Even Want Gamification?' (Colorado Technical University, 2023).

In the literature addressing the use of gamification in cybersecurity education, the developed areas of cybersecurity knowledge are quite diverse. These range from strong passwords, sensitive data security, phishing, physical security, clickjacking, online privacy, social engineering, spear-phishing, vishing, smishing, baiting, tailgating, malware, virus, cyberbullying, cyberstalking, identify theft, worms, denial of service, to hijacking.

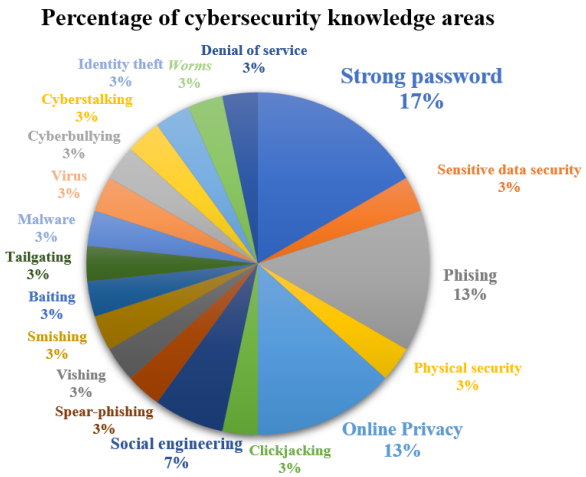

Figure 3. Percentage of developed cybersecurity knowledge areas in the literature

As illustrated in Figure 3, the literature analysis reveals that the most frequently developed cybersecurity knowledge area using gamification is strong passwords, accounting for 17%. This is followed by phishing and online privacy, each with a percentage of 13%, and social engineering with 7%. Meanwhile, other cybersecurity knowledge areas, such as sensitive data security, physical security, clickjacking, online privacy, spear-phishing, vishing, smishing, baiting, tailgating, malware, virus, cyberbullying, cyberstalking, identity theft, worms, denial of service, and hijacking, each have a percentage of 3%.

Gamification is closely linked to elements that serve to actively engage students and evoke emotional responses in the learning process[37]. The gamification elements utilized vary significantly in the analyzed literature, encompassing time intervals, points, leaderboards, goals, rules, competition, badges, levels, tasks, hints, rewards, cards, matching, memory, achievements, streaks, challenges, nudging, and roles.

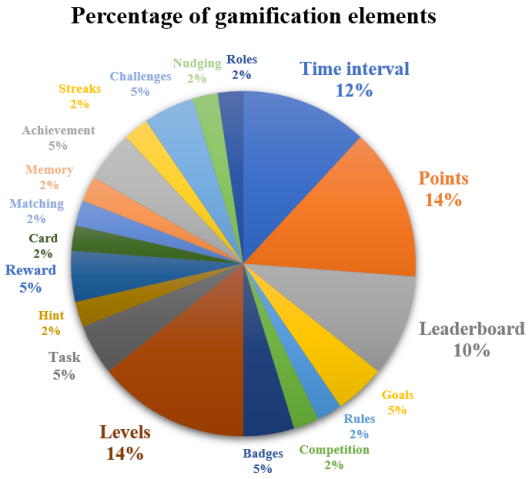

Figure 4. Percentage of utilized gamification elements in the literature

As shown in Figure 4, among all the gamification elements analyzed in the literature, points and levels exhibit the highest percentage, each at 14%. Following closely, time intervals have a percentage of 12%, and leaderboards have a percentage of 10%. Goals, badges, tasks, rewards, achievements, and challenges each account for a 5% percentage, while rules, competition, hints, cards, matching, memory, streaks, nudging, and roles each contribute to a 2% percentage.

The results of this investigation uncover how gamification is employed to enhance students' comprehension of crucial cybersecurity topics. Gamification elements like points and levels facilitate student competition, making them widely utilized to craft engaging and motivational learning experiences. The inclusion of time intervals in gamification introduces a challenging aspect with time constraints, encouraging students to think and act swiftly in cybersecurity-related scenarios. Additionally, the implementation of leaderboards allows students to monitor their rankings, motivating them to attain higher scores. The prevalent game elements identified in the reviewed literature encompass points, levels, time

[37] Karl M. Kapp, *The Gamification of Learning and Instruction: Game-Based Methods and Strategies for Training and Education* (John Wiley & Sons, 2012).

intervals, and leaderboards. These findings align with DeCarlo's viewpoint, asserting that competitive and conflict elements in gamification stimulate student engagement in the learning process [38]. Furthermore, in line with Kapp's research, it is evident that integrating motivating elements such as time intervals and challenges that allow for failure leads to increased retention in learning[39]. Gamification elements play a crucial role in motivating students and delivering an effective learning experience, especially in the realm of cybersecurity education. The cybersecurity knowledge areas highlighted in the literature under study include strong passwords, phishing, online privacy, and social engineering. The importance of strong password knowledge is stressed by Qusa and Tarazi, who argue that students need education regarding the significance of strong passwords to safeguard themselves from cyber threats [40]. Moreover, Scholefield and Shepherd underscore that passwords serve as the primary authentication mechanism for accessing cyber services, underscoring the need for users to maintain secure passwords. In their research, Scholefield and Shepherd observed a 5% increase in cybersecurity knowledge, particularly in the strong password area, facilitated by the use of gamification [41]. According to the reviewed literature, the integration of gamification in cybersecurity education proves to be effective in broadening and deepening students' comprehension of various cybersecurity aspects, crucial in today's digital world. By incorporating appropriate gamification elements, this method has the potential to cultivate a generation with a heightened knowledge of cybersecurity, prepared to confront the increasingly diverse cybersecurity threats in the future.

Analysis of Cybersecurity Knowledge Areas, CIA Aspects, Threat and Attack Categories of Cybersecurity Education in the Literature

In the reviewed literature, gamified cybersecurity education provides a more in-depth understanding of various cybersecurity knowledge aspects, encompassing potential threats and attacks that may compromise the CIA aspects (Confidentiality, Integrity, and Availability) of information security. The classification of threats or attacks, based on the studied cybersecurity knowledge areas and their impact on CIA aspects, is presented in Table 2.

Table 2. Classification of knowledge areas, CIA aspects, threat or attack categories based on reviewed literature

Knowledge area	CIA aspects that are attacked or threatened	Threat or attack categories
Hacking due to weak passwords	Confidentiality, Integrity	Passive threat
Data theft	Confidentiality	Passive threat
Phishing	Confidentiality	Active threat
Physical security risk	Availability	Active threat
Hacking and data theft	Confidentiality, Integrity	Passive threat
Clickjacking	Confidentiality, Integrity	Active threat
Social engineering	Confidentiality	Active threat
Spear-phishing	Confidentiality	Active threat
Vishing	Confidentiality	Active threat
Smishing	Confidentiality	Active threat
Baiting	Confidentiality	Active threat
Tailgating	Confidentiality, Integrity, Availability	Active threat
Malware	Confidentiality, Integrity, Availability	Active threat
Virus	Confidentiality, Integrity, Availability	Active threat
Cyberbullying	Confidentiality	Active threat
Cyberstalking	Confidentiality	Active threat
Identity theft	Confidentiality, Integrity	Active threat
Worms	Confidentiality, Integrity, Availability	Active threat
Denial of services	Availability	Passive attack
Hijacking	Confidentiality, Integrity	Active threat

According to this classification, the resulting percentages, illustrated in Figure 5, reveal that among all the threats and attacks within the analyzed cybersecurity knowledge areas in the

[38] DeCarlo.
[39] Kapp.
[40] Qusa and Tarazi.
[41] Schole and Shepherd.

literature, 55% pose a threat to Confidentiality, 27% to Integrity, and 18% to Availability. These percentages reflect the complex dynamics of challenges encountered in the cyber realm. Notably, the heightened attention to the Confidentiality aspect indicates a noteworthy trend in cyberattacks.

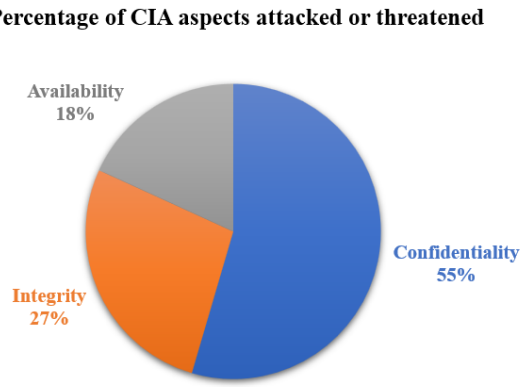

Figure 5. Percentage of CIA aspects attacked or threatened based on cybersecurity knowledge areas in the literature

The high percentage related to the Confidentiality aspect highlights its crucial role in the realm of cybersecurity. This significance stems from the substantial value associated with confidential information, making it a potential target for unauthorized access. Confidential information can encompass sensitive data, trade secrets, personal details, and more, all carrying the risk of being exploited for various harmful purposes. Most confidential information misuse often involves motives such as criminal activities, commercial interests, and hate speech, all of which can inflict damage on the reputation of individuals or organizations [42]. Hence, a comprehensive understanding of the imperative nature of safeguarding information confidentiality becomes a vital component in the cybersecurity education knowledge area. This ensures that students gain insight into the complex challenges associated with information confidentiality and acquire knowledge of effective protection strategies.

Furthermore, based on the classification provided in Table 2, the obtained percentages, illustrated in Figure 6 below, reveal that out of the 19 cybersecurity knowledge areas reviewed in the literature, 95% are categorized as threats, while 5% are identified as attacks. More than 50%, and nearly 100%, of the total literature reviewed, emphasizes areas falling within the realm of cybersecurity threats.

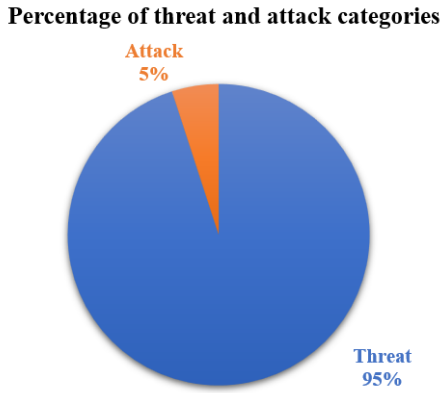

Figure 6. Percentage of threat and attack categories based on cybersecurity knowledge areas in the literature

This shows that there is a greater emphasis on cybersecurity education addressing threats through gamification, as opposed to areas focusing on cybersecurity attacks. Cybersecurity education holds paramount importance for individuals especially students, who may still be unfamiliar with the landscape of cybercrime. It equips them with the knowledge needed to counter various forms of cyber threats prevalent in today's digital era. By understanding cybersecurity threats, students will take preventive measures to recognize the potential risks of attacks.

In addition, as depicted in Figure 7 below, 80% of all cybersecurity knowledge areas covered in the literature are categorized as active threats, 15% fall under passive threats, and 5% are passive attacks. Both active attacks and advanced attacks have a percentage of 0%.

[42] Nurhasanah Nurhasanah and Indra Rahmatullah, 'Financial Technology and the Legal Protection of Personal Data: The Case of Malaysia and Indonesia', *Al-Risalah: Forum Kajian Hukum Dan Sosial Kemasyarakatan*, 20.2 (2020), 197–214 <https://doi.org/10.30631/al-risalah.v20i2.602>.

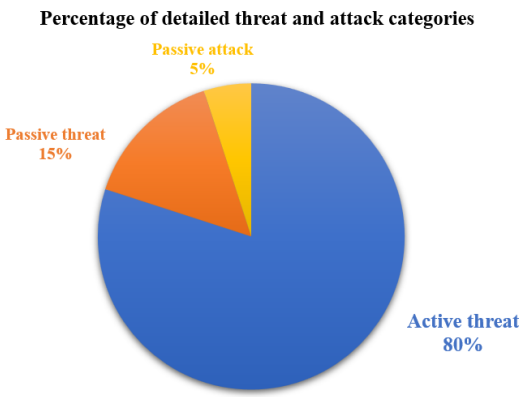

Figure 7. Percentage of detailed threat and attack categories based on cybersecurity knowledge areas in the literature

This illustrates that areas addressing active cybersecurity threats are more extensively incorporated into cybersecurity education through gamification in comparison to areas discussing passive threats, active attacks, passive attacks, and advanced attacks. Active threats encompass foundational cybersecurity principles, making cybersecurity education emphasizing active cybersecurity threats an important measure to equip students with the knowledge to protect their information and data in the risk-filled digital world. The high percentage of active cybersecurity threat knowledge areas in cybersecurity education is crucial for minimizing preventable cybercrime actions.

Analysis of Gamification Elements and CIA Aspects in Cybersecurity Education in Literature

The comprehensive analysis results provide a classification of gamification elements and trained CIA aspects, as presented in the following Table 3.

Table 3. Classification of gamification elements and trained CIA aspects

Gamification element	Confidentiality	Integrity	Availability
Time interval	✓	✓	✓
Points	✓	✓	
Leaderboard	✓	✓	✓
Goals	✓	✓	
Rules	✓	✓	
Competition	✓	✓	
Badges	✓	✓	
Levels	✓	✓	✓
Task	✓	✓	
Hint	✓	✓	
Reward	✓	✓	✓
Card	✓		✓
Matching	✓		✓
Memory	✓		✓
Achievements	✓	✓	
Streaks	✓	✓	
Challenges	✓	✓	
Nudging	✓	✓	
Roles	✓	✓	

This categorization reveals that the gamification elements utilized to train and enhance the confidentiality aspect of cybersecurity include time intervals, points, leaderboards, goals, rules, competitions, badges, levels, tasks, hints, rewards, cards, matching, memory, achievements, streaks, challenges, nudging, and roles. For training and enhancing the integrity aspect of cybersecurity, the gamification elements encompass time intervals, points, leaderboards, goals, rules, competition, badges, levels, tasks, hints, rewards, achievements, streaks, challenges, nudging, and roles. As for training and boosting the availability aspect of cybersecurity, the gamification elements consist of time intervals, leaderboards, levels, rewards, cards, matching, and memory. Based on this classification, it can be inferred that gamification elements like points, goals, rules, competition, badges, tasks, hints, achievement, streaks, challenges, nudging, and roles effectively address confidentiality and integrity but not the availability aspect. Gamification elements such as card, matching, and memory prove effective in training confidentiality and availability but not integrity.

Discussion

Appropriate Gamification Elements Based on CIA Aspects in Cybersecurity Education for Recent Threats and Attacks

The persistent evolution of cybersecurity threats and attacks remains a critical concern on both a global scale and specifically within Indonesia, reflecting the ever-changing landscape of technology. The trends in cyber threats and

attacks not only continue to evolve but also grow in complexity and diversity. Consequently, staying informed about the latest trends and proactively anticipating potential threats that might dominate in the future becomes imperative. As technology advances, it opens up opportunities for cyber attackers to identify system vulnerabilities and compromise sensitive data. Recent cyber threats and attacks have gained prominence and are anticipated to remain focal points in the foreseeable future. Moreover, closely monitoring emerging developments in the cybersecurity area is crucial. The ongoing evolution of cyber threats and attacks underscores the necessity of sustained cybersecurity efforts to ensure the protection of vital data and information in the years ahead.

Referring to the BSSN (*Badan Siber dan Sandi Negar*a) report during the early-year press conference held at the BSSN office in South Jakarta on Monday (20/2/2023), several categories of cybersecurity threats and attacks are exhibiting notable trends and are anticipated to be focal points. These include data breaches, advanced persistent threats, diverse phishing attacks on the rise, crypto-jacking, and distributed denial of service. Furthermore, cybercrimes through the Internet of Things (IoT) and Artificial Intelligence (AI) are emerging as potential threats that will evolve in the future[43]. Additionally, as outlined by Bondan Estuwira, the Head of the Cybersecurity and Crypto Task Force for the North Sulawesi region within the Cyber and Crypto Security Agency of BSSN, during the Cyber and Crypto Security Review for the *Komisi Pemilihan Umum Daerah* (KPUD) in North Sulawesi on Thursday (25/10/2023), he outlined that credential leaks stand out as a crucial cybersecurity threat that requires careful monitoring and serious attention. This is imperative for securing cybersecurity against potential threats and vulnerabilities during the execution of the 2024 elections[44]. According to the security advisory released by BSSN on Saturday (28/01/2023), it draws attention to a recent phishing variant involving Android-based applications (.apk) impersonating Wedding Invitation Letters, presenting a significant threat in the current cybersecurity landscape [45]. Additionally, the Federal Bureau of Investigation (FBI) in the US has issued alerts regarding new trends in double ransomware attacks since July 2023[46]. Table 4 below provides a categorization of the latest types of threats and attacks, their classifications, and the CIA aspects they pose a threat.

Table 4. Classification of types of threats and attacks, categories, and CIA aspects attacked or threatened

Types of threats and attacks	Categories of threats and attacks	CIA aspects attacked or threatened
Data breach	Passive threat	Confidentiality
Advanced persistent threat	Advance attack	Confidentiality, Integrity, Availability
Phishing with latest variations: android based application	Active threat	Confidentiality, Integrity, Availability
Crypto-jacking	Active threat	Integrity, Availability
Distributed denial of service	Passive attack	Availability
Artificial Intelligence dan Internet of things cybercrime	Active threat	Confidentiality, Integrity, Availability
Leak credential	Passive threat	Confidentiality, Integrity
Dual ransomware	Active threat	Confidentiality, Integrity, Availability

[43] Biro Hukum dan Komunikasi Publik, 'Terbitkan Annual Report Berisi Prediksi Ancaman Siber 2023, BSSN: Materi Literasi Budaya Keamanan Siber Dan Buktikan Akuntabilitas Kinerja', 2023 <https://www.bssn.go.id/annualreport2022/> [accessed 5 November 2023].

[44] Biro Hukum dan Komunikasi Publik, 'Ancaman Siber Makin Kompleks Jelang Pemilu 2024, BSSN Reviu Keamanan Siber Dan Sandi Pada KPUD Sulawesi Utara', 2023 <https://www.bssn.go.id/ancaman-siber-makin-kompleks-jelang-pemilu-2024-bssn-reviu-keamanan-siber-dan-sandi-pada-kpud-sulawesi-utara/> [accessed 5 November 2023].

[45] Kementerian Komunikasi dan Informatika, 'Aplikasi Undangan Pernikahan Digital', 2023 <https://www.kominfo.go.id/content/detail/47121/hoaks-aplikasi-undangan-pernikahan-digital/0/laporan_isu_hoaks> [accessed 5 November 2023].

[46] The Hacker News, 'FBI Warns of Rising Trend of Dual Ransomware Attacks Targeting U.S. Companies', 2023 <https://thehackernews.com/2023/09/fbi-warns-of-rising-trend-of-dual.html> [accessed 5 November 2023].

Several potential cybersecurity threats and attacks are currently noteworthy and are predicted to be major concerns in the future. These encompass data breaches, advanced persistent threats, phishing with recent variations, crypto-jacking, distributed denial of service, artificial intelligence and Internet of things cybercrime, credential leaks, and double ransomware.

Data breaches as passive threats, occur when attackers try to access or steal sensitive or confidential data without the knowledge or permission of the data owner. In certain cases, they may only attempt to extract this data without being detected. Data breach threats can lead to severe security breaches, resulting in significant financial and reputational impacts on organizations or individuals who become victims. Attackers exploiting data breaches pose a threat to the confidentiality aspect as they steal information such as personal details, financial records, business plans, or other sensitive information [47]. An advanced persistent threat attack is a large-scale cyber assault targeting significant infrastructure or entities, aiming to obtain sensitive information, especially concerning specific company security systems including confidentiality, integrity, and availability [48]. The recent form of active threat phishing involves attackers using fake Android Package Kit (.apk) files, tricking victims into downloading them. In this phishing scenario, if the victim installs the application, it requests Short Message Service (SMS) access, providing the attacker with the victim's mobile banking username and password from data leaks. When logging into mobile banking, the app sends a One Time Password (OTP) via SMS, readable by the attacker through the installed application. Unauthorized access to the victim's financial information threatens confidentiality, integrity, and availability [49]. The active threat of crypto-jacking is a new strategy for illegal entry to the victim's computer, utilizing its computing power for cryptocurrency mining, negatively impacting computer performance and posing a cyber threat, especially in terms of integrity and availability[50]. Passive distributed denial of service attacks occur when a considerable number of compromised computers or devices controlled by attackers are employed to send a target with an extensive volume of data traffic, this leads to overwhelming the target, causing operational disruptions [51]. DDoS attacks pose a threat to the availability aspect [52], rendering online services or websites inaccessible to legitimate users. The active cybercrime threat involving artificial intelligence (AI) and the Internet of Things (IoT) involves criminal actions utilizing AI technology and IoT devices. The range of these threats encompasses aspects like confidentiality, integrity, and availability [53]. The range of these threats

[47] Monica Gadre, 'Data Security in Cloud Security Attacks and Preventive Measures', *International Journal for Research in Applied Science and Engineering Technology*, 6.3 (2018), 529–36 <https://doi.org/10.22214/ijraset.2018.3085>.

[48] Irshad Ahmed Sumra, Halabi Bin Hasbullah, and Jamalul Lail Bin AbManan, 'Attacks on Security Goals (Confidentiality, Integrity, Availability) in VANET: A Survey', *Advances in Intelligent Systems and Computing*, 306.June 2014 (2015), 51–61 <https://doi.org/10.1007/978-981-287-158-9_5>.

[49] Natasha M Wojcicki, 'Phishing Attacks: Preying on Human Psychology to Beat the System and Developing Cybersecurity Protections to Reduce the Risks.', *World Libraries*, 23.1 (2019), 1–14 <https://widgets.ebscohost.com/prod/customerspecific/ns000545/customproxy.php?url=https://search.ebscohost.com/login.aspx?direct=true&db=lxh&AN=143379093&amp%0Alang=pt-pt&site=eds-live&scope=site>.

[50] Subhan Ullah and others, 'Prevention of Cryptojacking Attacks in Business and FinTech Applications', *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications*, 2022, 266–87 <https://doi.org/10.4018/978-1-6684-5284-4.ch014>.

[51] Nadila Sugianti and others, 'Deteksi Serangan Distributed Denia of Services (DDOS) Berbasis HTTP Menggunakan Metode Fuzzy Sugeno', *JISKA (Jurnal Informatika Sunan Kalijaga)*, 4.3 (2020), 18 <https://doi.org/10.14421/jiska.2020.43-03>.

[52] Raj Kumar Patel, Dr. Lalan Kumar Singh, and Dr. Narendra Kumar, 'Literature Review of Distributed: Denial of Service Attack Protection', *International Journal for Research in Applied Science and Engineering Technology*, 11.1 (2023), 1032–36 <https://doi.org/10.22214/ijraset.2023.48673>.

[53] Murat Kuzlu, Corinne Fair, and Ozgur Guler, 'Role of Artificial Intelligence in the Internet of Things

encompasses aspects like confidentiality, integrity, and availability. Examples include the unauthorized access of personal data through susceptible IoT devices, hacking attacks on smart home automation systems, or the use of AI to enhance the efficiency of cyberattacks. With the rapid advancement of these technologies, cybercrime involving AI and IoT becomes increasingly relevant, necessitating stronger preventive measures and protection. Passive threats of credential leakage occur when login details or security information, including usernames and passwords, from an account or system are exposed to unauthorized entities. This information may leak through various means, such as website hacking, security vulnerabilities, or fraudulent activities. When credentials are leaked, jeopardizing confidentiality and integrity, cybercriminals can exploit the situation to gain unauthorized access to the victim's account or system[54]. This poses a significant cybersecurity risk, potentially resulting in data theft, fraudulent activities, or unauthorized access to sensitive information. The active threat of ransomware with this new variant involves a dual ransomware attack, where the attacker encrypts the victim's data and demands a ransom for the decryption key. In dual ransomware threats, attackers not only threaten to restore access to the victim's data but may also threaten additional consequences if the ransom is not paid. In certain cases, dual ransomware attackers might threaten to disclose or sell the encrypted data to others if the ransom is not paid. this introduces complexity and heightened impact to ransomware attacks, as the victim's confidential, integrity, and availability aspects are put at risk[55].

Based on the identified correlation through classification in Table 3, the author can summarize the gamification elements applicable to cybersecurity education, posing a threat to the CIA Triad. This is visually represented in the author's crafted Venn diagram, illustrated in Figure 8 below.

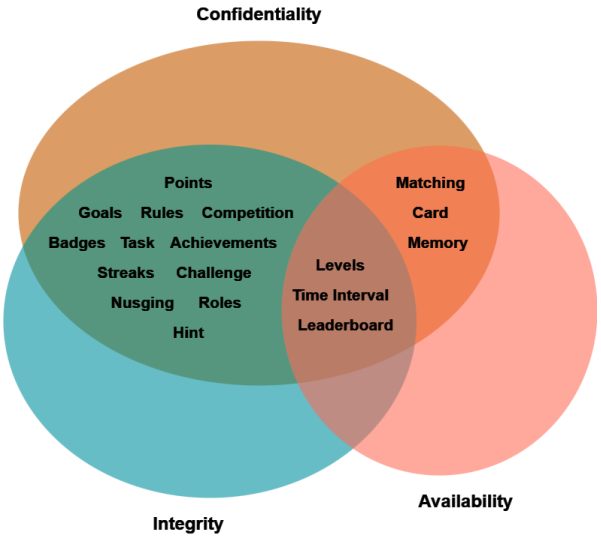

Figure 8. Venn diagram illustrating the alignment of gamification elements with the CIA Triad aspects

In this diagram, the region within the orange and green circles signifies gamification elements well-suited for cybersecurity education attacking confidentiality and integrity aspects. The area encompassed by the orange, green, and red circles indicates gamification elements fitting for cybersecurity education attacking confidentiality, integrity, and availability aspects. The area within the orange and red circles represents gamification elements suitable for cybersecurity education attacking confidentiality and availability aspects.

In summary, gamification elements suitable for educating about cybersecurity in data breaches includes points, goals, rules, competition, badges, task, achievements, streaks, challenges, nudging, roles, hint, levels, time interval, leaderboards, matching, card, and memory. Notably, the use of points and badges in gamification aligns with Bellekens et al's recommendation for enhancing awareness in the context of data breach threats[56]. Gamification

(IoT) Cybersecurity', *Discover Internet of Things*, 1.1 (2021) <https://doi.org/10.1007/s43926-020-00001-4>.

[54] Mitsuaki Akiyama, Takeshi Yagi, and Kazufumi Aoki, 'For Observing Web-Based Attack Cycle', 2013, 223–43.

[55] Siddharth Routray, Debachudamani Prusti, and Santanu Kumar Rath, *Ransomware Attack Detection by Applying Machine Learning Techniques*, *Lecture Notes in Electrical Engineering* (Springer Nature Singapore, 2023), 997 LNEE <https://doi.org/10.1007/978-981-99-0085-5_62>.

[56] Xavier Bellekens and others, *From Cyber-Security Deception to Manipulation and Gratification Through Gamification*,

elements appropriate for educating about advanced persistent threats in cybersecurity encompass points, goals, rules, competition, badges, tasks, achievements, streaks, challenges, nudging, roles, hints, levels, time intervals, leaderboard, matching, card, and memory. This aligns with Nicho's findings that introducing challenging elements like competition and time intervals is vital for advanced persistent threat cybersecurity awareness[57]. Gamification elements suitable for educating about the recent phishing variants in cybersecurity encompass points, goals, rules, competition, badges, task, achievements, streaks, challenges, nudging, roles, hint, levels, time interval, leaderboard, matching, card, and memory. This aligns with the findings of Tchakounté et al. and Arachchilage & Hameed, which recommend the use of gamification elements such as points, task, achievements, hint, levels, time interval, and leaderboard to enhance awareness in this cybersecurity knowledge area[58,59]. Gamification elements appropriate for educating about cybersecurity in crypto jacking include points, goals, rules, competition, badges, task, achievements, streaks, challenges, nudging, roles, hint, levels, time interval, leaderboard, matching, card, and memory. This is consistent with the findings of Priya & Ranganathan, who observed positive responses to the implementation of gamification elements like points, hint, levels, and cards in cybersecurity learning focused on crypto jacking awareness[60]. Additionally, the suggestion by Vekaria et al. that challenging elements should be integrated in this area reinforces this conclusion[61]. Gamification elements well-suited for educating on cybersecurity in distributed denial of service attacks comprise levels, time interval, leaderboard, matching, card, and memory. This aligns with Harilal's findings, recommending gamification elements that heighten tension and competition, such as time intervals and leaderboards, for awareness in this area of cybersecurity knowledge[62]. For cybercrime education involving Artificial Intelligence and the Internet of Things, appropriate gamification elements include points, goals, rules, competition, badges, task, achievements, streaks, challenges, nudging, roles, hint, levels, time interval, leaderboard, matching, card, and memory. Specifically, gamification elements like points, levels, leaderboards align with research by Ntsama et al. and Wijaya et al., advocating for these elements in raising awareness about cybercrime involving Artificial Intelligence and the Internet of Things[63,64]. Gamification elements fitting for educating about cybersecurity in leak

Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Springer International Publishing, 2019), 11594 LNCS <https://doi.org/10.1007/978-3-030-22351-9_7>.

[57] Mathew Nicho, 'Gam-Apt: A Serious Game Attribute Taxonomy for Advanced Persistent Threats', section V, 2020, 61–68 <https://doi.org/10.33965/ac2020_202013l008>.

[58] Franklin Tchakounté, Leonel Kanmogne Wabo, and Marcellin Atemkeng, 'A Review of Gamification Applied to Phishing', March, 2020, 1–26 <https://doi.org/10.20944/preprints202003.0139.v1>.

[59] Nalin Asanka Gamagedara Arachchilage and Mumtaz Abdul Hameed, 'Integrating Self-Efficacy into a Gamified Approach to Thwart Phishing Attacks', 2017 <http://arxiv.org/abs/1706.07748>.

[60] P Mohana Priya and Abhijit Ranganathan, 'Cyber Awareness Learning Imitation Environment (CALIE): A Card Game to Provide Cyber Security Awareness for Various Group of Practitioners', *International Journal of Advanced Networking and Applications*, 14.2 (2022), 5334–41

[61] Komal Bhupendra Vekaria and others, 'Cyber Range for Research-Inspired Learning of "Attack Defense by Pretense" Principle and Practice', *IEEE Transactions on Learning Technologies*, 14.3 (2021), 322–37 <https://doi.org/10.1109/TLT.2021.3091904>.

[62] Athul Harilal and others, 'The Wolf of SUTD (TWOS): A Dataset of Malicious Insider Threat Behavior Based on a Gamified Competition', *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 9.1 (2018), 54–85 <https://doi.org/10.22667/JOWUA.2018.03.31.054>.

[63] JE Ntsama, C Fachkha, and PB Owomo, 'A Gamification Architecture to Enhance Phishing Awareness', *Researchgate.Net*, September, 2023 <https://www.researchgate.net/profile/Claude-Fachkha-2/publication/374053419_A_Gamification_Architecture_to_Enhance_Phishing_Awareness/links/650afbb8c05e6d1b1c1ef6b0/A-Gamification-Architecture-to-Enhance-Phishing-Awareness.pdf>.

[64] William Wijaya and others, 'Gamified Tailored Roleplay Story-Based Phishing Awareness Training', *International Journal of Data Science and Advanced Analytics*, 4 (2018), 146–53.

credential include points, goals, rules, competition, badges, task, achievements, streaks, challenges, nudging, roles, hint, levels, time interval, leaderboard, matching, card, and memory. This aligns with research by Hartwig et al. and Amft et al., which recommends gamification elements like points, competition, achievement, dan challenge for enhancing awareness in the leak credential threat area[65,66]. Gamification elements suitable for educating on dual ransomware in cybersecurity include points, goals, rules, competition, badges, task, achievements, streaks, challenges, nudging, roles, hint, levels, time interval, leaderboard, matching, card, and memory. Notably, the incorporation of challenges as a gamification element aligns with Lika et al's perspective, emphasizing its use to foster significant commitment in students learning about the complexities of dual ransomware[67] and encouraging them to persist despite encountering failures[68]. Additionally, given the social engineering aspect of dual ransomware, the utilization of gamification elements like roles is recommended in this specific knowledge area[69].

Conclusion

In this research, the author conducted a thorough literature review following specific criteria, resulting in the identification of 13 articles indexed on Google Scholar, published between 2018 and 2023, focusing on the application of gamification methods in cybersecurity education for students. The research originated from the urgent need driven by increased internet usage and the complexity of cyber threats in the current digital era, emphasizing the critical importance of cybersecurity knowledge in education, the concept of gamification, enriched with various elements and acknowledged as a progressively effective method not only across disciplines but also in crucial knowledge areas, emerged as a fitting choice for implementation. Further exploration of gamification utilization in cybersecurity education, based on prior research, offered valuable insights. The research concluded by pinpointing gamification elements aligned with each aspect of the CIA Triad (Confidentiality, Integrity, Availability) facing threats. This conclusion serves as a roadmap for crafting in navigating the evolving landscape of cybersecurity threats, requiring profound comprehension and serious preventive measures.

Through this research, it is evident that gamification elements hold significant potential for improving cybersecurity education, especially in dealing with the increasingly complex nature of contemporary threats and attacks. By comprehending the correlation between gamification elements and the aspects of the CIA Triad, educators can design more targeted and adaptable learning strategies to meet students' needs. For future research, can investigate the impact of utilizing gamification with the suggested elements on enhancing students' comprehension and skills in confronting cybersecurity threats and attacks. Expanding the scope of this research is expected to offer a more comprehensive and relevant insight for the future development of cybersecurity education tailored for students.

[65] Katrin Hartwig and others, 'Finding Secret Treasure? Improving Memorized Secrets through Gamification', *ACM International Conference Proceeding Series*, 2021, 105–17 <https://doi.org/10.1145/3481357.3481509>.

[66] Sandra Höltervennhoff and Nicolas Huaman, "' Would You Give the Same Priority to the Bank and a Game ? I Do Not !" Exploring Credential Management Strategies and Obstacles during Password Manager Setup This Paper Is Included in the Proceedings of the Nineteenth Symposium on Usable Privacy and Secu', 2023.

[67] Reyner Aranta Lika and others, 'NotPetya: Cyber Attack Prevention through Awareness via Gamification', *2018 International Conference on Smart Computing and Electronic Enterprise, ICSCEE 2018*, 2018, 1–6 <https://doi.org/10.1109/ICSCEE.2018.8538431>.

[68] Andrea Continella and others, 'ShieldFS: A Self-Healing, Ransomware-Aware File System', *ACM International Conference Proceeding Series*, 5-9-Decemb (2016), 336–47 <https://doi.org/10.1145/2991079.2991110>.

[69] Ana Ferreira, 'Why Ransomware Needs A Human Touch', *Proceedings - International Carnahan Conference on Security Technology*, 2018-Octob (2018), 1–5 <https://doi.org/10.1109/CCST.2018.8585650>.

References

Books

Bell, David, *An Introduction to Cybercultures* (Routledge, 2006)

Kapp, Karl M., *The Gamification of Learning and Instruction: Game-Based Methods and Strategies for Training and Education* (John Wiley & Sons, 2012)

Keen, Andrew, *The Internet Is Not the Answer* (Atlantic Books Ltd, 2015)

Riyanarto Sarno, Irsyat Iffano, *Sistem Manajemen Keamanan Informasi* (Surabaya: ITS Press, 2009)

Werbach, Kevin, and Dan Hunter, 'For the Win: How Game Thinking Can Revolutionize Your Business: 9781613630235: Amazon.Com: Books', *Universadad de Pensylvania*, 2012, 146 <https://www.amazon.com/Win-Game-Thinking-Revolutionize-Business/dp/1613630239/ref=pd_sim_14_3?_encoding=UTF8&psc=1&refRID=4FRM3MYBDM74G24R5R8Q>

Journals

Abu, Md Sahrom, Siti Rahayu Selamat, Aswami Ariffin, and Robiah Yusof, 'Cyber Threat Intelligence – Issue and Challenges', *Indonesian Journal of Electrical Engineering and Computer Science*, 10.1 (2018), 371–79 <https://doi.org/10.11591/ijeecs.v10.i1.pp371-379>

Akiyama, Mitsuaki, Takeshi Yagi, and Kazufumi Aoki, 'For Observing Web-Based Attack Cycle', 2013, 223–43

Alothman, Basil, Khaznah Al-Khulifa, Reem Al-Shammari, Chibli Joumaa, and Murad Khan, 'Towards Enhancing Cyber Security Awareness Using Gamification Escape Room', *International Conference on Ubiquitous and Future Networks, ICUFN*, 2023-July (2023), 828–30 <https://doi.org/10.1109/ICUFN57995.2023.10199673>

Arachchilage, Nalin Asanka Gamagedara, and Mumtaz Abdul Hameed, 'Integrating Self-Efficacy into a Gamified Approach to Thwart Phishing Attacks', 2017 <http://arxiv.org/abs/1706.07748>

Bellekens, Xavier, Gayan Jayasekara, Hanan Hindy, Miroslav Bures, David Brosset, Christos Tachtatzis, and others, *From Cyber-Security Deception to Manipulation and Gratification Through Gamification*, *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Springer International Publishing, 2019), 11594 LNCS <https://doi.org/10.1007/978-3-030-22351-9_7>

Benedikt, Michael, 'Introduction to Cyberspace: First Steps', *Cyberspace: First Steps*, 1991, 458 <https://archive.org/details/CyberspaceFirstSteps/mode/2up>

Brady, Callum, and Andrew M'Manga, 'Gamification of Cyber Security Training-EnsureSecure', *Proceedings - 2022 IEEE International Conference on e-Business Engineering, ICEBE 2022*, 2022, 7–12 <https://doi.org/10.1109/ICEBE55470.2022.00010>

Broholm, Rasmus, Michael Christensen, and Lene Tolstrup Sorensen, 'Exploring Gamification Elements to Enhance User Motivation in a Cyber Security Learning Platform Through Focus Group Interviews', *Proceedings - 7th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2022*, 2022, 470–76 <https://doi.org/10.1109/EuroSPW55150.2022.00056>

Continella, Andrea, Alessandro Guagnelli, Giovanni Zingaro, Giulio De Pasquale, Alessandro Barenghi, Stefano Zanero, and others, 'ShieldFS: A Self-Healing, Ransomware-Aware File System', *ACM International Conference Proceeding Series*, 5-9-Decemb (2016), 336–47 <https://doi.org/10.1145/2991079.2991110>

DeCarlo, Sean M, 'Measuring the Application of Knowledge Gained from the Gamification of Cybersecurity Training in Healthcare', May, 2020, 90 <https://search.proquest.com/docview/2461612243/abstract/C50CBA5A6DB14D3CPQ/1%0Ahttps://media.proquest.com/media/hms/PFT/2/9z0ZH?cit%3Aauth=DeCarlo%2C+Sean+M.&cit%3Atitle=Measuring+the+Application+of+Knowledge+Gained+from+the+Gamification+...&cit%3Apub=Pro>

Diakoumakos, Jason, Evangelos Chaskos, Nicholas Kolokotronis, and George Lepouras, 'Cyber-Range Federation and

Cyber-Security Games: A Gamification Scoring Model', *Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience, CSR 2021*, 2021, 186–91 <https://doi.org/10.1109/CSR51186.2021.9527972>

Fatokun Faith, B., Zalizah Awang Long, Suraya Hamid, O. Fatokun Johnson, Christopher Ifeanyi Eke, and Azah Norman, 'An Intelligent Gamification Tool to Boost Young Kids Cybersecurity Knowledge on FB Messenger', *Proceedings of the 2022 16th International Conference on Ubiquitous Information Management and Communication, IMCOM 2022*, 2022 <https://doi.org/10.1109/IMCOM53663.2022.9721733>

Ferreira, Ana, 'Why Ransomware Needs A Human Touch', *Proceedings - International Carnahan Conference on Security Technology*, 2018-Octob (2018), 1–5 <https://doi.org/10.1109/CCST.2018.8585650>

Fleischman, Katja, and Ellen Ariel, 'Gamification in Science Education: Gamifying Learning of Microscopic Processes in the Laboratory', *Contemporary Educational Technology*, 7.2 (2020), 138–59 <https://doi.org/10.30935/cedtech/6168>

Gabriel˙e Kvietinskait˙e, Linas Bukauskas, and Virgilijus Krinickij, 'Cyber Security Table-Top Exercise Gamification with Dynamic Scenario for Qualification Assessment', *Springer*, 1654 (2022), 54–62 <https://doi.org/https://doi.org/10.1007/978-3-031-19679-9_8>

Gadre, Monica, 'Data Security in Cloud Security Attacks and Preventive Measures', *International Journal for Research in Applied Science and Engineering Technology*, 6.3 (2018), 529–36 <https://doi.org/10.22214/ijraset.2018.3085>

Gjertsen, Eyvind Garder B., Erlend Andreas Gjære, Maria Bartnes, and Waldo Rocha Flores, 'Gamification of Information Security Awareness and Training', *ICISSP 2017 - Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, 2017-Janua.January (2017), 59–70 <https://doi.org/10.5220/0006128500590070>

Hamdan, Zainab, Iman Obaid, Asma Ali, Hanan Hussain, Amala V. Rajan, and Jinesh Ahamed, 'Protecting Teenagers from Potential Internet Security Threats', *Proceedings of the 2013 International Conference on Current Trends in Information Technology, CTIT 2013*, 2013, 143–52 <https://doi.org/10.1109/CTIT.2013.6749493>

Harilal, Athul, Flavio Toffalini, Ivan Homoliak, John Castellanos, Juan Guarnizo, Soumik Mondal, and others, 'The Wolf of SUTD (TWOS): A Dataset of Malicious Insider Threat Behavior Based on a Gamified Competition', *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 9.1 (2018), 54–85 <https://doi.org/10.22667/JOWUA.2018.03.31.054>

Hartwig, Katrin, Atlas Englisch, Jan Pelle Thomson, and Christian Reuter, 'Finding Secret Treasure? Improving Memorized Secrets through Gamification', *ACM International Conference Proceeding Series*, 2021, 105–17 <https://doi.org/10.1145/3481357.3481509>

Höltervennhoff, Sandra, and Nicolas Huaman, '" Would You Give the Same Priority to the Bank and a Game ? I Do Not !" Exploring Credential Management Strategies and Obstacles during Password Manager Setup This Paper Is Included in the Proceedings of the Nineteenth Symposium on Usable Privacy and Secu', 2023

Indrajit, R E, 'Enam Aspek Menjaga Dan Melindungi Dunia Maya', … *(Internet and Infrastructure/Coordination Center)* …, 2017 <https://www.academia.edu/download/33264299/Aspek_menjaga_dan_melindungi_dunia_maya.pdf>

Kim, Jung Tae, and Won Hyung Lee, 'Dynamical Model for Gamification of Learning (DMGL)', *Multimedia Tools and Applications*, 74.19 (2015), 8483–93 <https://doi.org/10.1007/s11042-013-1612-8>

Kuzlu, Murat, Corinne Fair, and Ozgur Guler, 'Role of Artificial Intelligence in the Internet of Things (IoT) Cybersecurity', *Discover Internet of Things*, 1.1 (2021) <https://doi.org/10.1007/s43926-020-

00001-4>

Lika, Reyner Aranta, Danushyaa Murugiah, Sarfraz Nawaz Brohi, and Daksha A.P.V. Ramasamy, 'NotPetya: Cyber Attack Prevention through Awareness via Gamification', *2018 International Conference on Smart Computing and Electronic Enterprise, ICSCEE 2018*, 2018, 1–6 <https://doi.org/10.1109/ICSCEE.2018.8538431>

Matovu, Richard, Joshua C. Nwokeji, Terry Holmes, and Tajmilur Rahman, 'Teaching and Learning Cybersecurity Awareness with Gamification in Smaller Universities and Colleges', *Proceedings - Frontiers in Education Conference, FIE*, 2022-Octob (2022), 1–9 <https://doi.org/10.1109/FIE56618.2022.9962519>

McClaskey, Tiffany M., 'Tabletop Exercises: Gamification in Cybersecurity', *ProQuest* (Utica University, 2022)

Mclaughlin, Kevin, 'A Quantitative Study of Learner Choice in Cybersecurity Training: Do They Even Want Gamification?' (Colorado Technical University, 2023)

Nicho, Mathew, 'Gam-Apt: A Serious Game Attribute Taxonomy for Advanced Persistent Threats', section V, 2020, 61–68 <https://doi.org/10.33965/ac2020_202013l008>

Nikander, Jussi, Onni Manninen, and Mikko Laajalahti, 'Requirements for Cybersecurity in Agricultural Communication Networks', *Computers and Electronics in Agriculture*, 179.September (2020), 105776 <https://doi.org/10.1016/j.compag.2020.105776>

Ntsama, JE, C Fachkha, and PB Owomo, 'A Gamification Architecture to Enhance Phishing Awareness', *Researchgate.Net*, September, 2023 <https://www.researchgate.net/profile/Claude-Fachkha-2/publication/374053419_A_Gamification_Architecture_to_Enhance_Phishing_Awareness/links/650afbb8c05e6d1b1c1ef6b0/A-Gamification-Architecture-to-Enhance-Phishing-Awareness.pdf>

Nurhasanah, Nurhasanah, and Indra Rahmatullah, 'Financial Technology and the Legal Protection of Personal Data: The Case of Malaysia and Indonesia', *Al-Risalah: Forum Kajian Hukum Dan Sosial Kemasyarakatan*, 20.2 (2020), 197–214 <https://doi.org/10.30631/al-risalah.v20i2.602>

Paryati, 'Keamanan Sistem Informasi', *Seminar Nasional Informatika 2008 (SemnasIF 2008) UPN 'Veteran' Yogyakarta, 24 Mei 2008*, 2008.semnasIF (2008), 379–86

Patel, Raj Kumar, Dr. Lalan Kumar Singh, and Dr. Narendra Kumar, 'Literature Review of Distributed: Denial of Service Attack Protection', *International Journal for Research in Applied Science and Engineering Technology*, 11.1 (2023), 1032–36 <https://doi.org/10.22214/ijraset.2023.48673>

Pawar, Mohan V., and J. Anuradha, 'Network Security and Types of Attacks in Network', *Procedia Computer Science*, 48.C (2015), 503–6 <https://doi.org/10.1016/j.procs.2015.04.126>

Priya, P Mohana, and Abhijit Ranganathan, 'Cyber Awareness Learning Imitation Environment (CALIE): A Card Game to Provide Cyber Security Awareness for Various Group of Practitioners', *International Journal of Advanced Networking and Applications*, 14.2 (2022), 5334–41 <http://0-search.proquest.com.www.elgar.govt.nz/scholarly-journals/cyber-awareness-learning-imitation-environment/docview/2734720451/se-2%0Ahttps://media.proquest.com/media/hms/PFT/1/fjIwP?_a=ChgyMDIyMTExNjE2NTQyMTYyMzoxMTc1NzcSBTU3MDYyGgpPTkVfU0VBUkNIIgwx>

Qusa, Hani, and Jumana Tarazi, 'Cyber-Hero: A Gamification Framework for Cyber Security Awareness for High Schools Students', *2021 IEEE 11th Annual Computing and Communication Workshop and Conference, CCWC 2021*, 2021, 677–82 <https://doi.org/10.1109/CCWC51732.2021.9375847>

Ricoy, María Carmen, and Cristina Sánchez-Martínez, 'Raising Ecological Awareness and Digital Literacy in Primary School Children through Gamification', *International Journal of Environmental Research and Public Health*, 19.3 (2022) <https://doi.org/10.3390/ijerph19031149>

Robson, Karen, Kirk Plangger, Jan H.

Kietzmann, Ian McCarthy, and Leyland Pitt, 'Is It All a Game? Understanding the Principles of Gamification', *Business Horizons*, 58.4 (2015), 411–20 <https://doi.org/10.1016/j.bushor.2015.03.006>

Routray, Siddharth, Debachudamani Prusti, and Santanu Kumar Rath, *Ransomware Attack Detection by Applying Machine Learning Techniques*, *Lecture Notes in Electrical Engineering* (Springer Nature Singapore, 2023), 997 LNEE <https://doi.org/10.1007/978-981-99-0085-5_62>

Schole, Sam, and Lynsay A Shepherd, 'Gami Fi Cation Techniques for Raising Cyber Security Awareness', 2019, 191–203 <https://doi.org/10.1007/978-3-030-22351-9>

Sugianti, Nadila, Yayang Galuh, Salma Fatia, and Khadijah Fahmi Hayati Holle, 'Deteksi Serangan Distributed Denia of Services (DDOS) Berbasis HTTP Menggunakan Metode Fuzzy Sugeno', *JISKA (Jurnal Informatika Sunan Kalijaga)*, 4.3 (2020), 18 <https://doi.org/10.14421/jiska.2020.43-03>

Sumra, Irshad Ahmed, Halabi Bin Hasbullah, and Jamalul Lail Bin AbManan, 'Attacks on Security Goals (Confidentiality, Integrity, Availability) in VANET: A Survey', *Advances in Intelligent Systems and Computing*, 306.June 2014 (2015), 51–61 <https://doi.org/10.1007/978-981-287-158-9_5>

Tchakounté, Franklin, Leonel Kanmogne Wabo, and Marcellin Atemkeng, 'A Review of Gamification Applied to Phishing', March, 2020, 1–26 <https://doi.org/10.20944/preprints202003.0139.v1>

Ullah, Subhan, Tahir Ahmad, Rizwan Ahmad, and Mudassar Aslam, 'Prevention of Cryptojacking Attacks in Business and FinTech Applications', *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications*, 2022, 266–87 <https://doi.org/10.4018/978-1-6684-5284-4.ch014>

Vekaria, Komal Bhupendra, Prasad Calyam, Songjie Wang, Ramya Payyavula, Matthew Rockey, and Nafis Ahmed, 'Cyber Range for Research-Inspired Learning of "Attack Defense by Pretense" Principle and Practice', *IEEE Transactions on Learning Technologies*, 14.3 (2021), 322–37 <https://doi.org/10.1109/TLT.2021.3091904>

Wahyudin, Yudin, and Dhian Nur Rahayu, 'Analisis Metode Pengembangan Sistem Informasi Berbasis Website: A Literatur Review', *Jurnal Interkom: Jurnal Publikasi Ilmiah Bidang Teknologi Informasi Dan Komunikasi*, 15.3 (2020), 26–40 <https://doi.org/10.35969/interkom.v15i3.74>

Wang, Qing, Zhenyu Chen, Junjie Wang, and Yang Feng, *Intelligent Crowdsourced Testing*, *Intelligent Crowdsourced Testing*, 2022 <https://doi.org/10.1007/978-981-16-9643-5>

Wijaya, William, Intan Farahana Kamsin, Zety Marlia, Zainal Abidin, Hemalata Vasudavan, Bukit Jalil, and others, 'Gamified Tailored Roleplay Story-Based Phishing Awareness Training', *International Journal of Data Science and Advanced Analytics*, 4 (2018), 146–53

Wojcicki, Natasha M, 'Phishing Attacks: Preying on Human Psychology to Beat the System and Developing Cybersecurity Protections to Reduce the Risks.', *World Libraries*, 23.1 (2019), 1–14 <https://widgets.ebscohost.com/prod/customerspecific/ns000545/customproxy.php?url=https://search.ebscohost.com/login.aspx?direct=true&db=lxh&AN=143379093&amp%0Alang=pt-pt&site=eds-live&scope=site>

Ypsilanti, Antonia, Ana B. Vivas, Teppo Räisänen, Matti Viitala, Tuula Ijäs, and Donald Ropes, 'Are Serious Video Games Something More than a Game? A Review on the Effectiveness of Serious Games to Facilitate Intergenerational Learning', *Education and Information Technologies*, 19.3 (2014), 515–29 <https://doi.org/10.1007/s10639-014-9325-9>

Yunus, Crystal Callista Anak, and Tan Kim Hua, 'Exploring a Gamified Learning Tool in the ESL Classroom: The Case of Quizizz', *Journal of Education and E-Learning Research*, 8.1 (2021), 103–8 <https://doi.org/10.20448/JOURNAL.509.2021.81.103.108>

Zainuddin, Zamzami, Muhammad Shujahat, Hussein Haruna, and Samuel Kai Wah Chu, 'The Role of Gamified E-Quizzes on Student Learning and Engagement: An Interactive Gamification Solution for a Formative Assessment System', *Computers and Education*, 145 (2020), 103729 <https://doi.org/10.1016/j.compedu.2019.103729>

Online References

Informatika, Kementerian Komunikasi dan, 'Aplikasi Undangan Pernikahan Digital', 2023 <https://www.kominfo.go.id/content/detail/47121/hoaks-aplikasi-undangan-pernikahan-digital/0/laporan_isu_hoaks> [accessed 5 November 2023]

News, The Hacker, 'FBI Warns of Rising Trend of Dual Ransomware Attacks Targeting U.S. Companies', 2023 <https://thehackernews.com/2023/09/fbi-warns-of-rising-trend-of-dual.html> [accessed 5 November 2023]

Publik, Biro Hukum dan Komunikasi, 'Ancaman Siber Makin Kompleks Jelang Pemilu 2024, BSSN Reviu Keamanan Siber Dan Sandi Pada KPUD Sulawesi Utara', 2023 <https://www.bssn.go.id/ancaman-siber-makin-kompleks-jelang-pemilu-2024-bssn-reviu-keamanan-siber-dan-sandi-pada-kpud-sulawesi-utara/> [accessed 5 November 2023]

———, 'Terbitkan Annual Report Berisi Prediksi Ancaman Siber 2023, BSSN: Materi Literasi Budaya Keamanan Siber Dan Buktikan Akuntabilitas Kinerja', 2023 <https://www.bssn.go.id/annualreport2022/> [accessed 5 November 2023]