**Learning Through Gaming: Developing a Mobile Serious Game on Cybersecurity for Primary School Students to Foster Sustainable Digital Literacy Skills**

**Abstract**

In the digital era, cybersecurity education has become indispensable. However, existing educational approaches often emphasize information literacy and foundational knowledge, with limited focus on cultivating sustainable digital literacy skills. To bridge this gap, this study developed a cybersecurity educational game targeted at elementary school students. The game aims to enhance students’ awareness of cybersecurity threats while fostering their skills in preventing and responding to such threats. The game scenarios simulate various cyber-attack situations, guiding students to think critically about identifying threats and implementing strategies to protect systems and data. This approach not only equips students with basic cybersecurity knowledge but also improves their defensive capabilities against potential cyber threats. The study employed a quasi-experimental design, dividing fifth-grade students into an experimental group (learning through mobile serious games) and a control group (traditional instruction). After the instruction phase, both groups were assessed for sustainable digital literacy skills and game self-efficacy. Results indicate that game-based learning enables students to actively construct cybersecurity knowledge, enhance learning interest, and increase engagement, thereby achieving sustainable learning outcomes. Future research could explore the effects of different game types on sustainable digital literacy skills and investigate how game design can optimize personalized learning experiences to comprehensively enhance students’ digital skills and competitiveness in the digital age.

Keywords: Mobile Serious Games, Cybersecurity Education, Sustainable Digital Literacy

1. **Introduction**

In modern education, the use of games and gamification techniques is gaining increasing attention, whether it involves imparting a vast amount of knowledge or cultivating students' practical skills in specific subjects. Gamified instruction requires the creation of a unique reality model governed by its own rules, such as role-playing games, business simulation games, or activity simulation games, to achieve educational objectives. This teaching approach is rooted in the research backgrounds of game-based learning (GBL) (Plass et al., 2015; Qian & Clark, 2016), simulation gaming (Crookall, 2010), and mobile learning (Jahnke et al., 2020), linking formal and informal education and bridging the gap between classroom learning and real-world applications (Alam, 2022). However, previous research has found that efforts to incorporate social networking sites (SNS) into the classroom are often limited to individual teachers' initiatives, lacking broader institutional implementation (Alam, 2022; Gumbheer et al., 2022), and have faced various challenges during experimentation. Firstly, although mobile devices offer communication and collaboration capabilities, real collaboration and engagement emerge from interpersonal interactions rather than merely relying on media or devices themselves (Shirky, 2014). Secondly, the majority of current classroom technology applications are still dominated by traditional information-driven models, which struggle to facilitate the knowledge production and construction that new media and tools can provide (Alam, 2021; Alam, 2022). Lastly, theoretical development and practical exploration by educators in this field remain insufficient. How to support in-service teachers in developing mobile learning experiences and how to utilize mobile resources to promote professional development are still areas requiring further research and practice (Yıldız et al., 2020).

To achieve the vision of collaborative learning and knowledge production brought about by new media and tools, a fundamental shift in educational philosophy and rules is essential. From educational policymakers to educators, all need to undergo re-education to establish innovative, student-centered, and collaborative teaching approaches. Bawa (2020) indicated that compared to traditional teaching methods, digital game-based learning can enhance learning outcomes and learner engagement. Unlike purely entertainment-focused games, educational games are designed with specific learning objectives and corresponding outcomes (Askarova & Jabborova, 2020). Social learning theory suggests that individuals learn from their environment through observation and interaction with others. This theory can be applied to the design of serious games, providing opportunities for social observation (Jeen et al., 2007) and role modeling (Fuchslocher et al., 2011). Constructivist learning theory posits that learning is an active process of constructing knowledge rather than passively acquiring it, and teaching should support this constructive process (Duffy, 1996). Under the framework of social constructivism, learning is a complex process involving learner development, the tools used, activities conducted, knowledge interaction, and personal learning beliefs (Cole, 1998; Ligorio, 2010; Vermunt & Verloop, 1999). These theoretical frameworks provide a solid foundation for developing mobile serious games for cybersecurity education, aiming to promote higher-order thinking and sustainable digital literacy skills.

The COVID-19 pandemic significantly altered our work and lifestyle, driving them toward the increased use of information and communication technology (ICT) and the internet (Ratten, 2020). However, there is a general lack of relevant digital literacy training, which affects learning and work outcomes related to ICT skills, critical thinking, and internet use (Ing et al., 2020). Nyikes (2018) pointed out that about 17% of young people fail to meet basic digital literacy requirements and need rapid improvement. Without proper digital literacy training, reliance on ICT and the internet for work and learning tasks poses greater risks when accessing online information, data, open-source applications, or uncertain programs. Educators also recognize that aspects of computational thinking (such as mathematics, statistics, data analysis, and critical thinking) are related to digital literacy and are currently considered educational goals in Taiwan (Gretter & Yadav, 2016). The goals of computational and critical thinking influence not only productivity but also the sustainability of personal and organizational development (Easterbrook, 2014). Technological advancements have been a major driver of global development in recent years, with ICTs providing users with unprecedented convenience and freedom (Caldwell, 2018; Kabakci et al., 2010; Rogers et al., 2014). However, users also face risks, such as internet addiction, information theft, and personal data exposure (Chen & He, 2013; Pomasunco & Orosco, 2020), including cyber addiction, information leakage, and personal information breaches (Alexei et al., 2021; Sikder et al., 2019). The goal of cybersecurity education is to educate users about potential risks when using online communication tools, such as social media, online games, email, and instant messaging. Although many studies on cybersecurity have been conducted across various fields, few have focused on cultivating cybersecurity awareness in schools (Rahman et al., 2020).

As society, markets, and technology continue to innovate, children’s use of the internet is rapidly evolving. Children frequently engage with online videos, music, games, messaging, and searches, generally indicating a positive use of the internet (OfCom, 2016). However, excessive internet use can lead to cyber risks, such as internet addiction, gaming and gambling addiction, cybersex, pornography exposure, and personal information leaks (Annansingh & Veli, 2016; Griffiths & Kuss, 2015; Hamid & Rahman, 2018). Cybercrimes targeting children and adolescents are a major concern for parents (Rahman et al., 2020), yet parents are often unaware that their children may be victims of cybercrime or even of the online activities their children are engaged in (Ahmad et al., 2018). This makes cybersecurity education an urgent and crucial task. Against this backdrop, this study develops a mobile serious game to promote elementary school students’ higher-order thinking skills and digital literacy, serving as an innovative and effective teaching method. Serious games combine entertainment and education, aiming to achieve educational goals through a gamified learning process. This approach not only captures students' attention but also facilitates learning and mastering cybersecurity knowledge through interaction and simulation, providing a pleasant experience. By facing various simulated cyber threats in the game, students learn relevant security knowledge while developing skills to analyze problems, devise strategies, and implement solutions.

In summary, in today’s digital and information-centric society, cybersecurity education is critical for elementary students. The development of mobile serious games not only promotes students' thinking skills, helping them tackle potential future cyber threats, but also enhances their digital literacy and fosters healthy, safe internet usage habits. Such an innovative educational approach contributes to a safer and more informed societal environment, providing a stronger foundation for the growth and development of the next generation. Digital game-based learning can take two primary forms. The first involves reusing existing educational games; however, this approach has clear limitations, as the content may not align well with specific curricula, and the game's entertainment aspects may negatively impact the educational process (Keller et al., 2024). Therefore, this study designs and develops games according to specific instructional content themes. This allows for accurate knowledge delivery, achievement of expected educational goals, and necessary balance among different game elements (Zhao, 2024). Based on this study, we propose the following research questions:

1. Can the game developed in this study promote students' sustainable digital literacy skills?
2. Does the game developed in this study enhance students’ perceived value of game self-efficacy?
3. **Literature review**
   1. **Serious Games on Mobile Learning**

Sotamaa (2007) defines serious games as activities governed by a set of established rules that players must follow to overcome specific challenges and achieve specific goals. In educational methods, serious games impart knowledge and experience to learners in an engaging manner (Damaševičius, 2014). The implementation of serious games has led to educational gamification, which is considered attractive and engaging for learners (Subhash & Cudney, 2018). These games repurpose video game technology originally used for entertainment toward more serious purposes, such as education, training, productivity, defense, and advertising. By integrating educational content into games, learning becomes both meaningful and enjoyable, thus increasing learners' intrinsic motivation and engagement (Kaczmarczyk et al., 2016). Mostafa & Faragallah (2019) describe serious games as interactive computer applications with challenging goals, regardless of the presence of significant electronic equipment. These games are fun and engaging, often incorporating scoring systems; they teach users skills, knowledge, or attitudes that can be applied in real-world contexts. Educational games are a branch of serious games, with Vargas et al. (2014) noting that over 60% of serious games are educational in nature. Unlike traditional teaching methods, games provide learners with a virtual space to practice and actively engage with learning topics without the pressures associated with formal learning (Zeng et al., 2020). Games elicit strong emotional responses in students and help them develop various skills and abilities, such as communication, teamwork, decision-making, and accountability. The gamification of education aims to make necessary conventional teaching content more vivid and engaging, serving as a beneficial complement to traditional educational forms. It helps ignite learners’ enthusiasm and better facilitates the implementation of collaborative learning methods (Plauska & Damaševičius, 2014).

Learning is an interactive process that connects learners' prior experiences with new knowledge (Hauge et al., 2017). Compared to other teaching methods, serious games have a competitive advantage due to their entertaining elements. A well-designed and successful serious game can enable learners to engage more effectively in the learning process, as the gaming experience offers entertainment value absent in other instructional approaches. Serious games gradually enhance learners’ contextual understanding, thereby strengthening learning outcomes (Kaczmarczyk et al., 2016). In many cases, serious games can increase players' motivation for both gaming and learning (Gros, 2007). These games encourage players to invest more time in learning. Participants engage their senses during gameplay, resulting in increased concentration and initiative to complete prescribed activities, effectively enriching the learning experience. Delgado et al. (2019) found that digital games are appealing to learners, and in learning environments, digital games can act as block-based games or game simulators to cultivate problem-solving skills. A distinctive aspect of digital games in education is the use of motion-sensing systems, which allow interaction with games through physical movements (Hung et al., 2018). Kosmas et al. (2018) also demonstrated how motion-sensing technology enhances embodied learning in teaching students with special educational needs. Embodied learning refers to an instructional approach that emphasizes non-cognitive factors in learning, focusing on body signals and sensations. Learners can develop new skills through various learning formats.

Numerous research papers have reported the positive learning outcomes and increased motivation brought about by serious games in promoting learning acquisition (Wouters et al., 2013). Many scholars argue that adopting game-based learning can be a more effective way to impart knowledge, particularly in subjects like mathematics and information technology (Kalmpourtzis, 2018). Other studies indicate that games involving physical movement can facilitate learning by enhancing the learning process and promoting learners’ health (Hung et al., 2018; Sapounidis et al., 2019). Gao and Mandryk (2012) found that motion-based game systems improve the cognitive and physical health of game learners. Orji et al. (2013) contributed by using motion-capture sensors in serious games. Some studies have used Kinect motion-sensing games, focusing on learner-centered approaches to develop cognitive, motor, and academic skills, achieving better learning outcomes (Kosmas et al., 2018; Kourakli et al., 2017). Beyond the benefits of learning, substantial work has also been done on the design of such games. For example, a multi-layered approach aids the game design process, enabling individuals involved in game design and game experiences to collaborate as a team to evaluate serious games. Emphasizing a collaborative framework enhances the engagement of designers and players, promoting research and analysis in serious game design (Slimani et al., 2016). Specifically, during the design phase of serious games, game designers, programmers, artists, and other domain experts need to collaborate to create an engaging computer-based learning game (Slimani et al., 2016; Mildner & ‘Floyd’ Mueller, 2016). However, implementing assessment in game-based learning environments still presents certain challenges.

Over the past decade, various assessment methods have been employed, such as conducting external measurements during gameplay, recording game data, or using other behavioral tests in non-game environments (Richey et al., 2021; Triantafyllou & Georgiadis, 2022; Zafeiropoulou et al., 2021). For serious games, some fundamental aspects that require careful consideration include game design, gameplay, and the experience gained. Additionally, when completing various learning tasks, game participants (designers, players, and experts) need to provide visual support for learners (Slimani et al., 2016). According to Self-Determination Theory, individual behavioral motivation primarily arises from three basic needs: autonomy, competence, and relatedness (Ryan et al., 2000). The need for autonomy refers to the opportunity for students to make independent choices during the learning process; the need for competence reflects students' desire to create effective behavior; and the need for relatedness emphasizes the importance of meaningful interactions among peers (Wang et al., 2019). Future research should further explore how to implement assessment methods in game-based learning environments that fulfill these three needs, thereby promoting genuine learning progress among students. Mobile serious games are highly interactive and flexible, enabling learning to take place anytime and anywhere. This learning approach is especially suitable for the lifestyle of modern students. Whether at home, school, or public places, as long as there is a mobile device and internet connection, students can engage in the game. This not only improves learning convenience but also increases student engagement and interest. Through continuous interaction and practice, students can reinforce their acquired knowledge and apply it in real-life situations, thereby achieving long-term outcomes.

* 1. **Gamified Sustainable Digital Literacy**

Koltay (2011) defines information literacy as user behaviors related to internet searching, hypertext navigation, knowledge synthesis, and content evaluation, while also reflecting users' awareness, attitudes, and abilities to use digital tools correctly, as well as their skills in identifying, acquiring, controlling, integrating, evaluating, analyzing, and synthesizing all digital resources. On this basis, users can construct new knowledge, create media expressions, and even enhance decision-making abilities (Ungerer, 2016). Literacy is not a new concept; it reflects individuals' social status, is used to establish connections with others or organizations, and is viewed as a form of cultural learning (Buckingham, 2010). Originating from the 2001 "No Child Left Behind" Act in the United States, educators’ focus shifted from skill development to literacy development (Ungerer, 2016). Literacy education plays a central role in modern education. In response to the rapid development of information and communication technology (ICT), information literacy is promoted as a new educational goal (Hatlevik et al., 2018). The internet is filled with a mix of true and false data, confusing users and even affecting societal development. Therefore, digital literacy has become a way to address the digital challenges posed by the evolution of ICT and internet usage (Jan, 2018).

Cybersecurity gamification is not a new topic, and many studies have been conducted on this subject in recent years (Hendrix et al., 2016). In the gamification design process for educational and training purposes, it is essential to clearly define specific training objectives (Caulkins et al., 2019). The goal of this study is to promote cybersecurity knowledge. Thus, team decision-making and collaboration are crucial for developing strong problem-solving skills, which can be easily translated into practical knowledge at the end of the learning process. In some cases, a storyline is needed to ensure a coherent and smooth gamification process. To design effective serious games, appropriate gamification elements must also be chosen to meet training method requirements (Caulkins et al., 2019). According to the literature, four gamification elements are suggested to facilitate the learning of cybersecurity knowledge. First is the progression mechanism, which involves motivating players by providing badges, leaderboards, and points as progress tools. The second is player control, which refers to using 2D or 3D characters that can participate in gamified training. Studies have shown that behavior can be influenced by diverse role-playing. The third is problem-solving, a crucial gamification element that must be integrated if the goal is to learn and retain new information. Finally, storylines create a narrative that establishes a bonding effect between virtual avatars and learners (Faith et al., 2024). The literature identifies three main aspects of cybersecurity gamification: foundational principles and awareness, defense strategies, and attack strategies. Foundational principles and awareness require participants to have a basic knowledge level, focusing on vulnerability assessments of entities and providing general knowledge to avoid and detect penetration attempts successfully. Defense strategies involve participants primarily acting as defenders, requiring them to master extensive knowledge to effectively use appropriate tools and strategies to counter cyberattacks. Attack strategies require participants in competitive scenarios to correctly understand basic methods and tactics. By centering on attackers, this training uses the established characteristics of cyber attackers to train users, predicting attackers' behaviors and motivations for specific tasks. This predictive approach enhances the application and creation of both defensive and offensive strategies against cyberattacks (Faith et al., 2024).

There are numerous examples in the literature of applying games to cybersecurity training, demonstrating their effectiveness. A notable example is CyberProtect, designed by information security administrators at the U.S. Department of Defense (Twitchell, 2007). In this game, players act as network administrators with limited budgets, tasked with purchasing equipment and providing proper training to protect their network from potential threats. The game is highly scalable, featuring scenarios like identity theft, worm prevention, and encrypted links, allowing players to gain experience in managing and mitigating cyber threats through problem-solving and critical thinking. Another significant example is CyberCIEGE, developed by the U.S. Naval Postgraduate School (Irvine et al., 2005). This game offers nearly 20 scenarios in a virtual world, requiring users to actively participate to protect their computer systems. It covers seven fundamental security-related topics, and its educational effectiveness has been validated in multiple studies (Cone et al., 2007; Jones et al., 2010), proving the value of games as learning tools. Also noteworthy is Anti-Phishing Phil, developed by Carnegie Mellon University, which teaches players to identify phishing attacks. Players assume the role of a fish, needing to determine whether worms in the ocean are phishing links (Sheng et al., 2007). Studies have shown that this game outperforms other educational materials in training effectiveness, significantly improving users' ability to identify phishing threats. In compliance with the U.S. Department of Defense regulations, all employees directly interacting with federal computer systems must participate in information security awareness training courses, leading to the development of the Cyber Awareness Challenge (Mostafa & Faragallah, 2019). Through this online game, participants learn security concepts and best practices for everyday work, applying their knowledge in scenario-based decision-making while encountering real threats like spyware, malicious code, and phishing. Lastly, the traditional Snakes and Ladders board game has been adapted to teach children proper and improper password handling methods (Reid & Van Niekerk, 2014). Research indicates that traditional games can be modified to incorporate information security concepts, effectively enhancing security awareness across different age groups and backgrounds, with a lasting impact on students' behaviors and awareness levels.

In summary, these examples illustrate the diverse approaches and proven effectiveness of applying serious games to cybersecurity training, promoting higher-order thinking and sustainable digital literacy skills. While the games mentioned above share some similarities with ours, they are mostly designed for other contexts, focusing on training specific security skills. Our primary goal is to apply educational games to elementary school cybersecurity education. As such, we cannot directly use the games mentioned in our study. Additionally, not all of these games are open-source, nor do they fully align with the pre-specified curriculum learning objectives. For these reasons, we chose to develop our own game to accurately serve the specified learning objectives, align with the curriculum content, and incorporate more learning theory aspects.

1. **Methodology**
   1. **Educational Game Model**

Learning styles (Rapeepisarn et al., 2008) and educational content (Prensky, 2005) are the two main factors determining the development of educational games. Learning style refers to the way students acquire information during the learning process, and an individual may adopt different learning styles. Since we aim to develop a game for teaching a large number of students, we need to identify a learning approach suitable for the majority of students. We modified the educational game model proposed by Mostafa & Faragallah (2019), as shown in Fig. 1. Sustainable digital literacy skills are set as the potential learning objectives and are integrated with cybersecurity knowledge points to form an educational game.

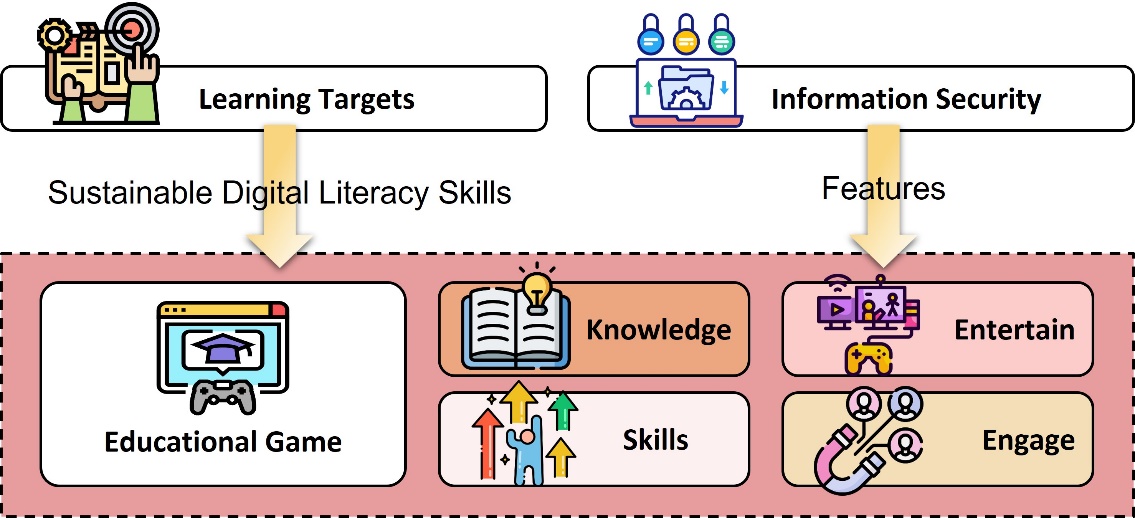


Fig 1. Educational Game Model Designed for This Study

This educational game not only entertains and engages learners but also helps them acquire knowledge and skills. Clearly, our educational game is designed to achieve specific learning objectives, defined as the “intrinsic integration of domain-specific learning within game mechanics and game world design” (Ke, 2017). These learning principles improve the gaming experience and are closely related to engagement principles (Marcelino et al., 2024). Therefore, we must first identify potential learning objectives and cybersecurity content. Then, we must determine the appropriate game types and features that support this content, achieving the necessary balance between learning and gaming (Kiili et al., 2005). Finally, when learners play a well-developed educational game, they develop their knowledge and skills through experience (Kolb et al., 2014). Hatzivasilis (2020) highlights the importance of practice in teaching. To acquire experience effectively, we must understand how knowledge is formed and which educational methods enhance learners’ experience acquisition (Hautamäki et al., 2019). Knowledge development and behavioral learning typically begin with instruction-based teaching. As learners' knowledge and skills improve, their “cognitive learning” also strengthens, which is then transitioned to a “constructivist learning” approach, primarily through exploratory learning and problem-based learning. The former involves responding to learning as a researcher (Israel et al., 2020), while the latter starts with solving practical problems and exploring relevant background information (Mann et al., 2021), leading to a deeper understanding of subject knowledge.

Some studies have also examined the integration of modern gamification techniques into the learning process (Jin et al., 2018; Švábenský et al., 2018). Scheponik (2016) studied college students in the field of cybersecurity, finding that achieving high levels of thinking and understanding is crucial. While students successfully completed related courses and grasped (cognitive learning) core concepts, they often misinterpreted the application of these core concepts (constructivist learning), such as distinguishing between confidentiality, integrity, or authentication (authorization). The impact of serious game topics is considered positive, yet psychological aspects are often overlooked in cybersecurity education. Taylor-Jackson (2020) investigated these issues, suggesting that factors like age, gender, or cultural background may make individuals more susceptible to malicious behaviors. Despite young people being familiar with technology, they may be more vulnerable to phishing emails than older individuals. Additionally, different types of learners have varying expectations of cybersecurity courses. For example, computer science students are primarily interested in how to conduct attacks, while psychology students focus on why someone might exploit vulnerabilities to harm systems or individuals. The general public, meanwhile, may be concerned about the side effects following a successful attack.

Other challenging issues include the “dynamism,” “workforce demand,” and “industry standards requirements” of computer science. Modern curriculum design must align seamlessly with the ever-evolving fields of computer science and cybersecurity (Shah et al., 2018). Therefore, in designing instructional models, it is crucial to identify learning methods preferred by the target audience (Rapeepisarn et al., 2008). Learners can play the game at their own pace and customize the rules according to their needs. Internet technology allows us to develop online educational games, offering scalable instructional solutions (Rutherford, 2014). Multiplayer games can also be developed to promote competition and socialization (Prensky, 2005). The vocabulary used in games must align with the underlying concepts of higher-order thinking skills, while the educational content must address current threat situations and provide positive feedback, such as professional certification, within the game (Knapp et al., 2017).

## Game Learning Material Design

Digital games have many enriching characteristics. Huang et al. (2013) point out that incorporating elements such as challenge, interactivity, entertainment, rule management, goal orientation, immersion in fantasy worlds, storytelling, engagement, and role-playing into educational games can make learning more enjoyable and effective. Playing digital games can enhance cognitive skills such as visual processing, attention, and spatial abilities (Bediou et al., 2018; Cardoso-Leite et al., 2020; Noroozi et al., 2020). Players are active participants in the learning process, encouraged to solve problems and create artifacts that demonstrate their acquired knowledge. Additionally, challenges and intrinsic rewards effectively motivate learners to engage and persist in completing learning tasks (Gee, 2005). Digital games possess this motivational effect for several reasons. First, digital games are fun and challenging, featuring structured rules and clear objectives (Wang et al., 2017). Second, they provide a flow experience without overloading cognitive abilities, such as working memory. Third, digital games offer immediate and continuous feedback, which stimulates player engagement. Fourth, they embed sequenced problems into storylines, making the learning process more captivating. Lastly, players can control their actions and personalize their gaming experience, further enhancing autonomy and involvement in learning (Gee, 2005).

In terms of educational content, games can be categorized into two major types: loosely connected and highly integrated contents. In loosely connected games, educational content does not directly influence game design. Instead, educational content is added on top of the game, as seen in image puzzles, quiz games, and traditional games. In contrast, highly integrated games, such as simulation games, role-playing games, and action/adventure games, treat educational content as a crucial component of game rules, storylines, and challenge design. Our developed game belongs to the latter category, where educational content is tightly integrated with game design (from rules and level narratives to potential learning objectives). Every player action and decision directly impacts the learning outcome. This means that the game mechanics must be designed to effectively teach cybersecurity concepts and ensure that players apply and reinforce this knowledge within the game. Regarding the choice of game dimensions, there is no consensus on the impact of game dimensions (2D/3D) on educational game effectiveness. Some studies suggest that 3D games can enhance student engagement and learning outcomes (Bai et al., 2012; Kebritchi et al., 2010), while others present alternative views (Ak & Kutlu, 2017; Schrader & Bastiaens, 2012). We believe that the choice of game dimension depends on various other factors, such as game mechanics, dynamics, aesthetics, and narrative. Therefore, this study employs Unity as the game development engine, given its rich features and wide adoption. The study follows Prensky’s (2005) theory and Rapeepisarn et al. (2008) research, aiming to establish connections among game types, learning strategies, and learning styles.

This study draws on the curriculum design method of Siddique et al. (2013), segmenting the course content into specific modules. The first step is to provide basic information: in this section, we design a module on the principles of DDoS attacks. Through visualization, players are introduced to the fundamental concepts of DDoS attacks, with cartoon characters replacing actual zombie viruses attacking the player. Players assume the role of an anthropomorphized computer, resisting the "zombie horde" to avoid infection and becoming part of it. In this phase, students need to understand and differentiate between different types of viruses, aligning with the critical thinking component of higher-order thinking skills. After providing the basic information, the game scenario presents players with clear encounter scenes, divided into two modules:

1. **DDoS Attack Techniques Module:** This module introduces players to common DDoS attack methods through a shooting game format. Different "attack ammunition," representing various DDoS techniques such as SYN Flood, UDP Flood, and HTTP Flood are launched, allowing players to observe and understand the impact of these attacks on network systems.
2. **DDoS Defense Module:** This module teaches players how to detect and defend against DDoS attacks, including setting up firewall rules, configuring load balancing, and using DDoS mitigation services.

In designing each level, we not only adhere to the previously mentioned guidelines but also follow the predetermined mechanics, opting for 3D as the game dimension. Each level provides basic cybersecurity knowledge to help players gradually understand the principles of DDoS attacks and enhance their cybersecurity awareness. Through the use of cartoon characters and interactive gameplay, players can learn how the "zombie horde" network forms and launches large-scale DDoS attacks on targets.

The game uses 3D simulations to represent the process of virus infection and computer control, progressively increasing the number of controlled computers to form a zombie horde. The horde can target different types of servers, such as web servers or game servers, launching large-scale attacks (access), visually demonstrating the impact on the servers. Players can set up firewalls through visual interfaces, using a shield to represent the protection offered by DDoS mitigation services. Isolation barriers and high-pressure water jets are used to simulate the process of cleansing attack traffic, as shown in Fig. 2. The types and intensities of attacks change throughout the levels, testing the players' adaptability. Based on defense effectiveness, players earn different scores and ratings, unlocking new defense equipment and scenarios upon level completion. Through simple and engaging attack-defense gameplay, players can experience the process of responding to DDoS attacks, understand the principles of various defense strategies, and improve their cybersecurity awareness and protective capabilities. Driven by curiosity, players engage in heuristic learning of the fundamentals of cybersecurity offense and defense.

|  |  |
| --- | --- |
|  |  |

Fig 2. Game Screenshots of Simulated Firewall and Traffic Scrubbing

* 1. **Experimental Procedure**

In this study, we invited a total of 84 fifth-grade students from an elementary school in southern Taiwan to participate. All students were divided into a control group (CG) and an experimental group (EG) for balanced comparison. The control group consisted of 42 students, as shown in Fig. 4, and employed traditional lecture-based teaching, using the National Cybersecurity Literacy Curriculum as the instructional content, with students completing learning tasks under the teacher's guidance. In contrast, the experimental group, also consisting of 42 students, used the aforementioned educational game as the instructional medium. The grouping was based on the enrollment semester to eliminate the influence of inherent characteristics and potential biases. The school administration and classroom teachers provided informed consent for participation and data collection, ensuring participant confidentiality and data anonymization throughout the study.

The study was applied to the senior-level information technology course in elementary school. At the start of the course, a pre-test was administered (Sustainable Digital Skills Scale and Game Self-Efficacy Scale). The initial phase of the course included a unified lecture to build a common foundational knowledge among students. Afterward, students were divided into the experimental and control groups as described above. The main difference between the two groups lay in the later stages of the teaching implementation. In the initial phase, both groups received the same foundational knowledge instruction, delivered by the same teacher to ensure consistency in teaching concepts. Upon course completion, the teacher presented predefined cybersecurity scenarios, developed in collaboration with the researchers, for group discussion. Students were asked to identify the type of technique, how to detect it, and the methods they would use to address it. A post- test was conducted at the end.

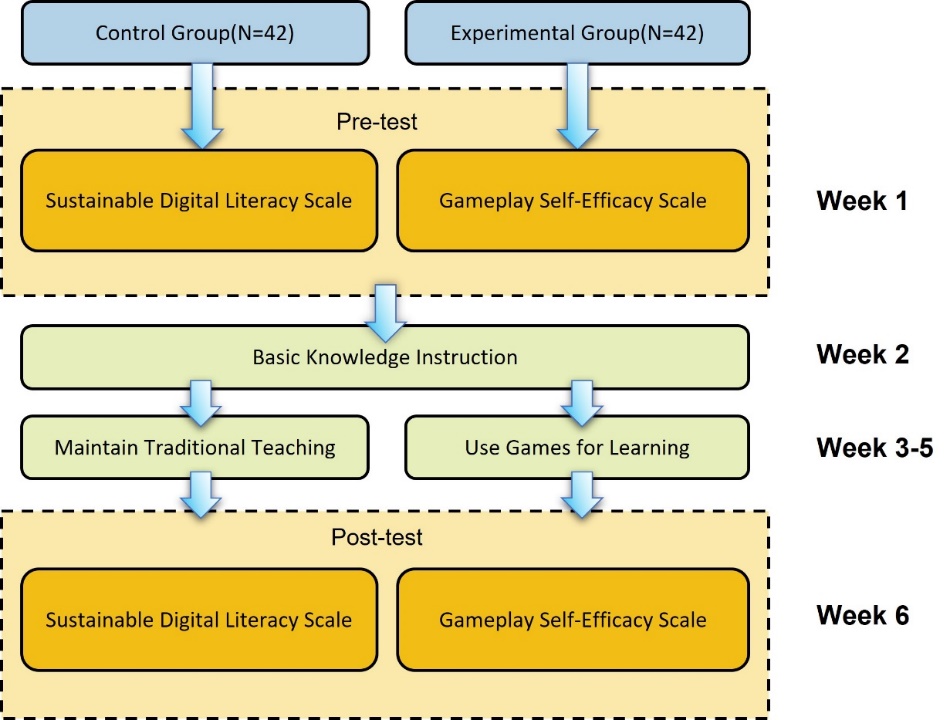


Fig 3. Research Flowchart

|  |  |
| --- | --- |
|  |  |

Fig 4. Experimental Group Course in Progress

1. **Experimental Questionnaire and Analysis**

A total of 84 questionnaires were collected in this study, with 42 participants each in the experimental and control groups. To address whether the game developed in this study could enhance students’ sustainable digital literacy skills, we adapted the Digital Literacy Scale designed by Sajidan et al. (2023) and the Online Social Behavior Scale proposed by Abdelraheem & Ahmed (2018) to create the Sustainable Digital Literacy Skills Scale used in this study. The dimensions of the Digital Literacy Scale (Sajidan et al., 2023) used are as follows: Use of Technology, which refers to familiarizing students with digital devices and related software, such as antivirus programs or browser settings, to improve their technical application skills; Information Management on Digital Media, which involves simulating real-life scenarios to help students identify and process real and valuable information; Online Safety, which focuses on teaching students how to protect personal data, avoid online threats (such as cyberbullying or malware), and handle inappropriate online content, thereby enhancing cybersecurity awareness; and Positive Impacts of Technology, which demonstrates the positive applications of digital technology in education and daily life. The scale provides a structured framework to comprehensively understand students' learning needs and growth potential in digital environments, guiding the design of educational activities that support their digital literacy development. In addition to staged knowledge acquisition, peer motivation and competition are also key factors in achieving sustainable learning outcomes.

The Online Social Behavior Scale (Abdelraheem & Ahmed, 2018) originally includes three dimensions: family relationships, social relationships, and social issue awareness. For this study, we adopted the latter two dimensions, believing that the development of sustainable digital literacy not only depends on the educational value of game design but also involves two critical aspects: the construction of peer social relationships and the enhancement of social responsibility awareness. Although the game primarily focuses on teaching defense against cyberattacks, its ultimate goal is to increase students’ awareness and vigilance about online safety. Through game-based learning, students can understand how to protect personal privacy on social media and other digital platforms, thus preventing potential cyber threats. We also encourage students to actively participate in and contribute to discussions and actions related to cybersecurity, supporting collective efforts in improving online safety. This not only helps build individual digital safety awareness but also fosters digital literacy and a culture of safety across society.

We used ANOVA to analyze the results, as shown in Table 1 and Table 2. Significant results were found in Use of Technology (F=84.53, *p* <.01), Online Safety (F=90.32, *p* <.01), Positive Impacts of Technology (F=81.23, *p* <.05), Social Relationships (F=76.45, *p* <.05), and Social Issue Awareness (F=73.24, *p* <.05). The findings support that game-based learning, particularly for cybersecurity education, not only improves students' understanding and awareness of cybersecurity but also encourages them to actively engage in discussions and actions related to online safety. This not only helps build individual digital safety awareness but also contributes to the development of a digital literacy and safety culture at a societal level. These factors interact to promote students' comprehensive development in sustainable digital literacy.

Table 1. ANOVA Analysis on Sustainable Digital Literacy Skills Scale

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| variable | SS | df | MS | F | *p* | Partial η2 |
| Use of Technology | 72.60 | 1 | 72.60 | 84.53 | 0.002\*\* | 0.496 |
| Information Management on  Digital Media | 69.83 | 1 | 0.84 | 69.83 | 0.54 | 0.010 |
| Online Safety | 146.86 | 1 | 146.83 | 90.32 | 0.009\*\* | 0.512 |
| Positive Impacts of Technology | 144.62 | 1 | 143.12 | 81.23 | 0.013\* | 0.486 |
| social relation | 147.27 | 1 | 147.27 | 76.45 | 0.043\* | 0.518 |
| social issues | 146.12 | 1 | 146.10 | 73.24 | 0.041\* | 0.501 |

Note. \**p* < .05, \*\**p* < .01, \*\*\**p* < .001

Table 2. Pre-test and Post-test Mean and Standard Deviation of the Sustainable Digital Literacy Skills Scale

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| variable | EG(N=42) | | | | CG(N=42) | | | |
| Pre-test | | Post-test | | Pre-test | | Post-test | |
| M | SD | M | SD | M | SD | M | SD |
| Use of Technology | 3.01 | 0.50 | 4.01 | 0.49 | 3.96 | 0.48 | 3.02 | 0.50 |
| Information Management on Digital Media | 3.00 | 0.48 | 3.10 | 0.49 | 3.02 | 0.47 | 3.03 | 0.46 |
| Online Safety | 2.17 | 0.49 | 4.02 | 0.51 | 3.01 | 0.50 | 3.03 | 0.41 |
| Positive Impacts of Technology | 3.03 | 0.33 | 4.03 | 0.50 | 3.54 | 0.49 | 3.04 | 0.73 |
| social relation | 2.73 | 0.49 | 4.01 | 0.50 | 3.00 | 0.25 | 3.02 | 0.48 |
| social issues | 3.02 | 0.48 | 4.02 | 0.49 | 3.41 | 0.50 | 3.03 | 0.24 |

Secondly, to explore the impact of the game developed in this study on students' game self-efficacy, we used ANOVA to analyze whether there were significant differences in the pre-test and post-test scores of the Game Self-Efficacy Scale. The scale, adapted from Hong et al. (2023), measures self-efficacy, which refers to an individual’s belief in their ability to successfully solve problems and complete tasks within a specific domain (Bandura, 1997). In addition to Gameplay Self-Efficacy, the scale also includes Gameplay Anxiety and Perceived Value. Gameplay anxiety describes a fluctuating emotional intensity; Spielberger (1972) distinguishes between state anxiety and trait anxiety, where state anxiety is a temporary feeling of tension, while trait anxiety refers to a predisposition to experience anxiety in various situations. When games introduce competitive elements, individuals may experience increased anxiety due to self-assessment of abilities and time constraints. Furthermore, an individual's expectations of success and perceived value of the activity influence their decision-making within the game.

Before conducting the ANOVA analysis on the pre-test and post-test scores of the Game Self-Efficacy Scale, we performed Levene’s test to verify homogeneity, which indicated that ANOVA could be performed (F=5.13, *p*=.624). Descriptive statistics and ANOVA results are shown in Table 4 and Table 5: students demonstrated a significant improvement in gameplay self-efficacy (F=45, *p* <.001, Partial η²=0.35), indicating a marked increase in their confidence to complete tasks during gameplay. This suggests that visual displays and repetitive training across different scenarios in the game helped students gradually enhance their skills and confidence. Gameplay Anxiety also showed a significant change (F=41.4, *p* <.001, Partial η²=0.333), suggesting that the pressure from varying scenarios and time constraints in the game allowed students to apply learned knowledge promptly, improving both memory retention and flexibility in applying knowledge to real-life situations. This design effectively promoted learning outcomes and improved application skills. Perceived Value also exhibited a significant change (F=24.48, *p* <.001, Partial η²=0.228), confirming that situational learning, compared to traditional education, not only facilitates learning but also makes the process more engaging and enjoyable.

Table 3. ANOVA Analysis on the Game Self-Efficacy Scale

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| variable | SS | df | MS | F | *p* | Partial η2 |
| Gameplay Self-Efficacy | 150 | 1 | 150 | 45 | <.001\*\*\* | 0.35 |
| Gameplay Anxiety | 133 | 1 | 132.88 | 41.4 | <.001\*\*\* | 0.333 |
| Perceived Value | 136.4 | 1 | 136.42 | 24.48 | <.001\*\*\* | 0.228 |

Note. \**p* < .05, \*\**p* < .01, \*\*\**p* < .001

Table 4. Pre-test and Post-test Mean and Standard Deviation of Self-Efficacy

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| variable | EG(N=42) | | | | CG(N=42) | | | |
| pretest | | posttest | | pretest | | posttest | |
| M | SD | M | SD | M | SD | M | SD |
| Gameplay Self-Efficacy | 15.3 | 1.91 | 21.8 | 3.01 | 15.4 | 1.6 | 22.5 | 3.08 |
| Gameplay Anxiety | 16.6 | 1.91 | 19.8 | 2.12 | 16.7 | 1.3 | 17.3 | 1.33 |
| Perceived Value | 12.8 | 1.92 | 15 | 2.39 | 12.5 | 2.1 | 12.5 | 2.46 |

1. **Discussion**

The current digital era requires individuals to possess the ability to recognize when information is needed and to effectively locate, evaluate, and utilize the necessary information, which is the core of information literacy (Irving, 2011). This study, through the design of a serious game, introduces information security in a visualized manner, emphasizing the concept of sustainable digital literacy beyond the foundation of information literacy. This concept not only encompasses the ability to locate, evaluate, and use information but also focuses on the ethical, environmental, and social impacts of information usage. For example, students’ social behaviors and online interactions are considered essential components of sustainable digital literacy. This literacy requires individuals to consider the broader impact of their behavior when handling and utilizing information, including how to interact responsibly and share information on online platforms. It is regarded as critical for the social, cultural, and economic development at national, community, institutional, and individual levels, necessitating deep knowledge, skills, and abilities (Whalen & Paez, 2021). To assess students’ capabilities in these areas, this study employed the Sustainable Digital Literacy Scale. Sustainability in learning is the core objective of achieving sustainable digital literacy, requiring students to be highly engaged and actively participate in the learning process. Moreover, given the constantly evolving nature of cybersecurity threats, students must continually learn and update their knowledge to effectively address increasingly complex online challenges. Therefore, we emphasize creating a research-based sustainable learning environment that helps students develop relevant knowledge and skills to better adapt to and handle these challenges (Owusu-Agyeman, 2021).

The study particularly focuses on the effectiveness of the developed game, concentrating on three dimensions within the scale: game self-efficacy, gameplay anxiety, and perceived value. These dimensions are commonly used to measure players’ psychological states and experiences during gameplay. Regarding the improvement of game self-efficacy, the results indicate that the serious game teaching, designed with varying scenarios and strategies, enabled students to invest more time and effort, leading to deeper learning and growth. Games are not only tools for entertainment but also effective learning media. When students successfully complete challenges and receive positive feedback in the game, their sense of self-efficacy is enhanced, increasing their confidence and engagement in other learning activities. Regarding gameplay anxiety, the study provides two interpretations. Moderate gameplay anxiety can stimulate excitement and a sense of challenge, prompting players to focus more on the game and strive to solve problems. However, excessive anxiety may negatively affect performance and learning outcomes, making it difficult for students to concentrate or even causing them to lose interest. This suggests that game designers need to balance challenges and pressure, ensuring that the game attracts players without causing excessive tension.

Lastly, the improvement in perceived value indicates that students’ overall evaluation of the game is positive, including their perceptions of the game’s content, experience, and educational value. Perceived value is closely related to the quality of game design, content relevance, and strategic requirements. When students find the game enjoyable and challenging, they are more willing to participate and engage in learning. High-quality game design can offer rich learning resources and diverse learning strategies, enabling students to understand and master the learning content from multiple perspectives. These findings suggest that the application of serious games in education not only enhances students’ self-efficacy and motivation but also improves their satisfaction with the learning process and outcomes. However, to maximize the educational value of games, designers need to carefully consider the scenarios and challenges within the game to balance motivation and pressure, ensuring a high degree of alignment between the game content and learning objectives. Future research could further explore how to optimize game design to promote the development of knowledge and skills across various learning environments.

1. **Conclusion and Future Work**

This study aims to explore how cybersecurity educational games can cultivate sustainable digital literacy skills among elementary school students. The developed game is designed to help students learn how to identify and respond to various cyber threats, such as denial-of-service attacks, Trojan viruses, and ransomware. The goal of the game design is to enable students to understand the nature of these threats and master related prevention and response strategies, thereby enhancing their sustainable digital literacy skills. Through game-based learning, students can apply the knowledge acquired to make informed judgments and responses when facing real-world cyber threats, showing significant improvements in critical thinking and problem-solving skills.

The study also identifies directions for future improvement. First, it could be beneficial to investigate how different types of games impact various aspects of sustainable digital literacy skills, to identify the most suitable game formats for developing diverse abilities. Second, further research could explore the mechanisms through which game-based learning affects sustainable education, investigating how to design games more effectively to enhance students’ digital literacy. Lastly, expanding the research to include students of different ages and backgrounds could help verify the universality and stability of the results.

In conclusion, this study confirms the potential of game-based cybersecurity education in enhancing elementary students' sustainable digital literacy skills, providing valuable references for future instructional design and application. Future efforts could focus on increasing game novelty or enhancing personalized learning experiences. Additionally, learning must be sustainable, which requires students to be highly engaged and actively involved. As cybersecurity threats continue to emerge and evolve, it becomes increasingly important to enhance students' digital literacy. Students need to continuously learn and update their knowledge to effectively address the growing complexity of cybersecurity challenges.

**References**

Abdelraheem, A. Y., & Ahmed, A. M. (2018). The Impact of Using Mobile Social Network Applications on Students' Social-Life. *International Journal of Instruction*, *11*(2), 1-14.

Ahmad, N., Asma’Mokhtar, U., Fauzi, W. F. P., Othman, Z. A., Yeop, Y. H., & Abdullah, S. N. H. S. (2018, November). Cyber security situational awareness among parents. In *2018 cyber resilience conference (crc)* (pp. 1-3). IEEE.

Ak, O., & Kutlu, B. (2017). Comparing 2D and 3D game‐based learning environments in terms of learning gains and student perceptions. *British Journal of Educational Technology*, *48*(1), 129-144.

Alam, A. (2021, November). Possibilities and apprehensions in the landscape of artificial intelligence in education. In *2021 International Conference on Computational Intelligence and Computing Applications (ICCICA)* (pp. 1-8). IEEE.

Alam, A. (2022). Cloud-based e-learning: scaffolding the environment for adaptive e-learning ecosystem based on cloud computing infrastructure. In *Computer Communication, Networking and IoT: Proceedings of 5th ICICC 2021, Volume 2* (pp. 1-9). Singapore: Springer Nature Singapore.

Alam, A. (2022). Impact of university’s human resources practices on professors’ occupational performance: empirical evidence from India’s higher education sector. In *Inclusive businesses in developing economies: Converging people, profit, and corporate citizenship* (pp. 107-131). Cham: Springer International Publishing.

Alam, A. (2022). Platform utilising blockchain technology for eLearning and online education for open sharing of academic proficiency and progress records. In *Smart Data Intelligence: Proceedings of ICSMDI 2022* (pp. 307-320). Singapore: Springer Nature Singapore.

Alexei, L. A., Nistiriuk, P., & Alexei, A. (2021). Empirical study of cyber security threats in Moldovan higher education institutions. In *Electronics, Communications and Computing* (pp. 241-244).

Annansingh, F., & Veli, T. (2016). An investigation into risks awareness and e-safety needs of children on the internet: a study of Devon, UK. *Interactive technology and smart education*, *13*(2), 147-165.

Askarova, U., & Jabborova, D. (2020). The Use of Game Technologies in Primary Education. *Am. J. Soc. Sci. Educ. Innov*, *2*, 478-485.

Bai, H., Pan, W., Hirumi, A., & Kebritchi, M. (2012). Assessing the effectiveness of a 3‐D instructional game on improving mathematics achievement and motivation of middle school students. *British Journal of Educational Technology*, *43*(6), 993-1003.

Bandura, A. (1997). *Self-efficacy: The exercise of control*. Macmillan.

Bawa, P. (2020). Game on!: Investigating digital game-based versus gamified learning in higher education. *International Journal of Game-Based Learning (IJGBL)*, *10*(3), 16-46.

Bediou, B., Adams, D. M., Mayer, R. E., Tipton, E., Green, C. S., & Bavelier, D. (2018). Meta-analysis of action video game impact on perceptual, attentional, and cognitive skills. *Psychological bulletin*, *144*(1), 77.

Buckingham, D. (2010). Defining digital literacy. Medienbildung in neuen Kulturräumen. *B. Bachmair (Ed.)*, 59-71.

Caldwell, H. (2018). Mobile technologies as a catalyst for pedagogic innovation within teacher education. *International Journal of Mobile and Blended Learning (IJMBL)*, *10*(2), 50-65.

Cardoso-Leite, P., Joessel, A., & Bavelier, D. (2020). 18 Games for Enhancing Cognitive Abilities. *Handbook of game-based learning*, 437.

Caulkins, B., Marlowe, T., & Reardon, A. (2019). Cybersecurity skills to address today’s threats. In *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity, July 21-25, 2018, Loews Sapphire Falls Resort at Universal Studios, Orlando, Florida, USA 9* (pp. 187-192). Springer International Publishing.

Chen, Y., & He, W. (2013). Security risks and protection in online learning: A survey. *International Review of Research in Open and Distributed Learning*, *14*(5), 108-127.

Cole, M. (1998). *Cultural psychology: A once and future discipline*. Harvard university press.

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *computers & security*, *26*(1), 63-72.

Crookall, D. (2010). Serious games, debriefing, and simulation/gaming as a discipline. *Simulation & gaming*, *41*(6), 898-920.

Damaševičius, R. (2014). Towards empirical modelling of knowledge transfer in teaching/learning process. In *Information and Software Technologies: 20th International Conference, ICIST 2014, Druskininkai, Lithuania, October 9-10, 2014. Proceedings 20* (pp. 359-372). Springer International Publishing.

Delgado, C., López, D. M., & Rico-Olarte, C. (2019, June). Affective video games: a systematic mapping study. In *International Conference on Human-Computer Interaction* (pp. 105-113). Cham: Springer International Publishing.

Duffy, T. M. (1996). Constructivism: Implications for the design and delivery of instruction. *Handbook of research for educational communications and technology*, 170-198.

Easterbrook, S. (2014, August). From Computational Thinking to Systems Thinking: A conceptual toolkit for sustainability computing. In *ICT for Sustainability 2014 (ICT4S-14)* (pp. 235-244). Atlantis Press.

Faith, B. F., Long, Z. A., & Hamid, S. (2024, May). Promoting cybersecurity knowledge via gamification: an innovative intervention design. In *2024 Third International Conference on Distributed Computing and High Performance Computing (DCHPC)* (pp. 1-8). IEEE.

Fuchslocher, A., Niesenhaus, J., & Krämer, N. (2011). Serious games for health: An empirical study of the game “Balance” for teenagers with diabetes mellitus. *Entertainment Computing*, *2*(2), 97-101.

Gao, Y., & Mandryk, R. (2012, May). The acute cognitive benefits of casual exergame play. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1863-1872).

Gee, J. P. (2005). Learning by design: Good video games as learning machines. *E-learning and Digital Media*, *2*(1), 5-16.

Gretter, S., & Yadav, A. (2016). Computational thinking and media & information literacy: An integrated approach to teaching twenty-first century skills. *TechTrends*, *60*, 510-516.

Griffiths, M. D., & Kuss, D. J. (2015). Online addictions: Gambling, video gaming, and social networking. *The handbook of the psychology of communication technology*, 384-403.

Gros, B. (2007). Digital games in education: The design of games-based learning environments. *Journal of research on technology in education*, *40*(1), 23-38.

Gumbheer, C. P., Khedo, K. K., & Bungaleea, A. (2022). Personalized and adaptive context-aware mobile learning: Review, challenges and future directions. *Education and Information Technologies*, *27*(6), 7491-7517.

Hamid, N. N. A., & Rahman, S. A. (2018). Impact of social media on Malaysia’s election landscape. *International Journal of Academic Research in Business and Social Sciences*, *8*(9), 275-284.

Hatlevik, O. E., Throndsen, I., Loi, M., & Gudmundsdottir, G. B. (2018). Students’ ICT self-efficacy and computer and information literacy: Determinants and relationships. *Computers & Education*, *118*, 107-119.

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., ... & Koshutanski, H. (2020). Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. *Applied Sciences*, *10*(16), 5702.

Hauge, J. M. B., Stefan, I. A., & Stefan, A. (2017). Exploring pervasive entertainment games to construct learning paths. In *Entertainment Computing–ICEC 2017: 16th IFIP TC 14 International Conference, Tsukuba City, Japan, September 18-21, 2017, Proceedings 16* (pp. 196-201). Springer International Publishing.

Hautamäki, J., Karjalainen, M., Hämäläinen, T., & Häkkinen, P. (2019). Cyber security exercise: Literature review to pedagogical methodology. In *INTED Proceedings* (No. 2019). IATED Academy.

Hendrix, M., Al-Sherbaz, A., & Victoria, B. (2016). Game based cyber security training: are serious games suitable for cyber security training?. *International Journal of Serious Games*, *3*(1), 53-61.

Hong, J. C., Hwang, M. Y., Hsu, H. T., & Tai, K. H. (2023). Gestalt perception: A game designed to explore players’ gameplay self-efficacy and anxiety reflected in their learning effects. *Journal of Research on Technology in Education*, *55*(3), 441-458.

Huang, W. D., Johnson, T. E., & Han, S. H. C. (2013). Impact of online instructional game features on college students’ perceived motivational support and cognitive investment: A structural equation modeling study. *The Internet and Higher Education*, *17*, 58-68.

Hung, J. W., Chang, Y. J., Chou, C. X., Wu, W. C., Howell, S., & Lu, W. P. (2018). Developing a suite of motion-controlled games for upper extremity training in children with cerebral palsy: a proof-of-concept study. *Games for health journal*, *7*(5), 327-334.

Ing, H. C., Yahaya, N., Laxman, K., & Al-Rahmi, W. M. (2020). Examining learners’ interaction pattern in asynchronous text-based online learning. *i-manager’s Journal of Educational Technology*, *16*(4), 9-19.

Irvine, C. E., Thompson, M. F., & Allen, K. (2005). CyberCIEGE: gaming for information assurance. *IEEE Security & Privacy*, *3*(3), 61-64.

Irving, C. (2011). National Information Literacy Framework (Scotland): Pioneering Work to Influence Policy Making or Tinkering at the Edges?. *library trends*, *60*(2), 419-438.

Israel, M., & Lash, T. (2020). From classroom lessons to exploratory learning progressions: Mathematics+ computational thinking. *Interactive Learning Environments*, *28*(3), 362-382.

Jahnke, I., Lee, Y. M., Pham, M., He, H., & Austin, L. (2020). Unpacking the inherent design principles of mobile microlearning. *Technology, Knowledge and Learning*, *25*, 585-619.

Jan, S. (2018). Investigating the Relationship between Students' Digital Literacy and Their Attitude towards Using ICT. *International Journal of Educational Technology*, *5*(2), 26-34.

Jeen, Y., Han, J., Kim, H., Lee, K., & Park, P. (2007). Persuasive interaction strategy for self diet system: Exploring the relation of user attitude and intervention by computerized systematic methods. In *Human-Computer Interaction. HCI Applications and Services: 12th International Conference, HCI International 2007, Beijing, China, July 22-27, 2007, Proceedings, Part IV 12* (pp. 450-458). Springer Berlin Heidelberg.

Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018). Evaluation of game-based learning in cybersecurity education for high school students. *Journal of Education and Learning (EduLearn)*, *12*(1), 150-158.

Jones, J., Yuan, X., Carr, E., & Yu, H. (2010, March). A comparative study of CyberCIEGE game and Department of Defense Information Assurance Awareness video. In *Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon)* (pp. 176-180). IEEE.

Kabakci, I., Ferhan Odabasi, H., & Kilicer, K. (2010). Transformative learning‐based mentoring for professional development of teacher educators in information and communication technologies: an approach for an emerging country. *Professional development in education*, *36*(1-2), 263-273.

Kaczmarczyk, J., Davidson, R., Bryden, D., Haselden, S., & Vivekananda‐Schmidt, P. (2016). Learning decision making through serious games. *The clinical teacher*, *13*(4), 277-282.

Kalmpourtzis, G. (2018). *Educational Game Design Fundamentals: A journey to creating intrinsically motivating learning experiences*. AK Peters/CRC Press.

Ke, F. (2017). Designing intrinsic integration of learning and gaming actions in a 3D architecture game. In *Handbook of research on serious games for educational applications* (pp. 234-252). IGI Global.

Kebritchi, M., Hirumi, A. & Bai, H. (2010). The effects of modern mathematics computer games on mathematics achievement and class motivation. *Computers & Education*, 55, 427–443.

Keller, T., Brucker-Kley, E., & Schwammel, P. (2024). A case study of an immersive learning unit for German as a second language. *Discover Education*, *3*(1), 28.

Kiili, K. (2005). Digital game-based learning: Towards an experiential gaming model. *The Internet and higher education*, *8*(1), 13-24.

Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance. *Journal of Information Systems Education*, *28*(2), 101.

Kolb, D. A., Boyatzis, R. E., & Mainemelis, C. (2014). Experiential learning theory: Previous research and new directions. In *Perspectives on thinking, learning, and cognitive styles* (pp. 227-247). Routledge.

Koltay, T. (2011). The media and the literacies: Media literacy, information literacy, digital literacy. *Media, culture & society*, *33*(2), 211-221.

Kosmas, P., Ioannou, A., & Retalis, S. (2018). Moving bodies to moving minds: A study of the use of motion-based games in special education. *TechTrends*, *62*(6), 594-601.

Kourakli, M., Altanis, I., Retalis, S., Boloudakis, M., Zbainos, D., & Antonopoulou, K. (2017). Towards the improvement of the cognitive, motoric and academic skills of students with special educational needs using Kinect learning games. *International Journal of Child-Computer Interaction*, *11*, 28-39.

Ligorio, M. B. (2010). Dialogical relationship between identity and learning. *Culture & Psychology*, *16*(1), 93-107.

Mann, L., Chang, R., Chandrasekaran, S., Coddington, A., Daniel, S., Cook, E., ... & Smith, T. D. (2021). From problem-based learning to practice-based education: A framework for shaping future engineers. *European Journal of Engineering Education*, *46*(1), 27-47.

Marcelino, L., Fernandes, P. M., & Cerqueira, J. (2024). Learning Engagement in a Pre-Alpha Version of an Educational Game: Evaluation and Proposed Solutions. *The International Journal of Games and Social Impact*, *2*(1), 28-45.

Mildner, P., & ‘Floyd’Mueller, F. (2016). Design of serious games. *Serious games: Foundations, concepts and practice*, 57-82.

Mostafa, M., & Faragallah, O. S. (2019). Development of serious games for teaching information security courses. *IEEE Access*, *7*, 169293-169305.

Noroozi, O., Dehghanzadeh, H., & Talaee, E. (2020). A systematic review on the impacts of game-based learning on argumentation skills. *Entertainment Computing*, *35*, 100369.

Nyikes, Z. (2018). Contemporary digital competency review. *Interdisciplinary Description of Complex Systems: INDECS*, *16*(1), 124-131.

OfCom, U. K. (2016). Children and parents: Media use and attitudes report. *London: Office of Communications London*.

Orji, R., Mandryk, R. L., Vassileva, J., & Gerling, K. M. (2013, April). Tailoring persuasive health games to gamer type. In *Proceedings of the sigchi conference on human factors in computing systems* (pp. 2467-2476).

Owusu-Agyeman, Y. (2021). Formation of a sustainable development ecosystem for Ghanaian universities. *International Review of Education*, *67*(3), 333-362.

Plass, J. L., Homer, B. D., & Kinzer, C. K. (2015). Foundations of game-based learning. *Educational psychologist*, *50*(4), 258-283.

Plauska, I., & Damaševičius, R. (2014). Educational robots for internet-of-things supported collaborative learning. In *Information and Software Technologies: 20th International Conference, ICIST 2014, Druskininkai, Lithuania, October 9-10, 2014. Proceedings 20* (pp. 346-358). Springer International Publishing.

Pomasunco, R., & Orosco, J. (2020). ‘Adolescents and risk of ICT. *Revista Electrónica de Investigación Educativa*, *22*(e17), 2-13.

Prensky, M. (2005). Computer games and learning: Digital game-based learning. *Handbook of computer game studies*, *18*(2005), 97-122.

Qian, M., & Clark, K. R. (2016). Game-based Learning and 21st century skills: A review of recent research. *Computers in human behavior*, *63*, 50-58.

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378-382.

Rapeepisarn, K., Wong, K. W., Fung, C. C., & Khine, M. S. (2008). The relationship between game genres, learning techniques and learning styles in educational computer games. In *Technologies for E-Learning and Digital Entertainment: Third International Conference, Edutainment 2008 Nanjing, China, June 25-27, 2008 Proceedings 3* (pp. 497-508). Springer Berlin Heidelberg.

Ratten, V. (2020). Coronavirus (covid-19) and entrepreneurship: changing life and work landscape. *Journal of Small Business & Entrepreneurship*, *32*(5), 503-516.

Reid, R., & Van Niekerk, J. (2014). Snakes and ladders for digital natives: information security education for the youth. *Information Management & Computer Security*, *22*(2), 179-190.

Richey, J. E., Zhang, J., Das, R., Andres-Bray, J. M., Scruggs, R., Mogessie, M., ... & McLaren, B. M. (2021, June). Gaming and confrustion explain learning advantages for a math digital learning game. In *International conference on artificial intelligence in education* (pp. 342-355). Cham: Springer International Publishing.

Rogers, E. M., Singhal, A., & Quinlan, M. M. (2014). Diffusion of innovations. In *An integrated approach to communication theory and research* (pp. 432-448). Routledge.

Rutherford, T., Farkas, G., Duncan, G., Burchinal, M., Kibrick, M., Graham, J., ... & Martinez, M. E. (2014). A randomized trial of an elementary school mathematics software intervention: Spatial-temporal math. *Journal of Research on Educational Effectiveness*, *7*(4), 358-383.

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American psychologist*, *55*(1), 68.

Sajidan, S., Atmojo, I., Desstya, A., Parmin, P., Saputri, D., & Salimi, M. (2023). The level of digital literacy ability of elementary school students. World Journal on Educational Technology: Current Issues. https://doi.org/10.18844/wjet.v15i1.8192.

Sapounidis, T., Demetriadis, S., Papadopoulos, P. M., & Stamovlasis, D. (2019). Tangible and graphical programming with experienced children: A mixed methods analysis. *International Journal of Child-Computer Interaction*, *19*, 67-78.

Scheponik, T., Sherman, A. T., DeLatte, D., Phatak, D., Oliva, L., Thompson, J., & Herman, G. L. (2016, October). How students reason about cybersecurity concepts. In *2016 IEEE Frontiers in Education Conference (FIE)* (pp. 1-5). IEEE.

Schrader, C., & Bastiaens, T. J. (2012). The influence of virtual presence: Effects on experienced cognitive load and learning outcomes in educational computer games. *Computers in Human Behavior*, *28*(2), 648-658.

Shah, V., Kumar, A., & Smart, K. (2018). Moving forward by looking backward: Embracing pedagogical principles to develop an innovative MSIS program. *Journal of Information Systems Education*, *29*(3), 139-156.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007, July). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 88-99).

Shirky, C. (2014). Why I just asked my students to put their laptops away. *Medium. com*, *11*.

Siddique, Z., Ling, C., Roberson, P., Xu, Y., & Geng, X. (2013). Facilitating higher-order learning through computer games. *Journal of Mechanical Design*, *135*(12), 121004.

Sikder, A. K., Aksu, H., & Uluagac, A. S. (2019). A context-aware framework for detecting sensor-based threats on smart devices. *IEEE Transactions on Mobile Computing*, *19*(2), 245-261.

Slimani, A., Elaachak, L., Elouaai, F., & Bouhorma, M. (2016, September). Evaluation-driven design for serious games, the multilayer methodology and collaborative framework. In *2016 8th International Conference on Games and Virtual Worlds for Serious Applications (VS-Games)* (pp. 1-3). IEEE.

Slimani, A., Yedri, O. B., Elouaai, F., & Bouhorma, M. (2016). Towards a design approach for serious games. *International Journal of Knowledge and Learning*, *11*(1), 58-81.

Sotamaa, O. (2007, January). Perceptions of player in game design literature. In *Proceedings of DiGRA 2007 Conference: Situated Play*.

Spielberger, Charles D. "Review of profile of mood states." (1972): 387.

Subhash, S., & Cudney, E. A. (2018). Gamified learning in higher education: A systematic review of the literature. *Computers in human behavior*, *87*, 192-206.

Švábenský, V., Vykopal, J., Cermak, M., & Laštovička, M. (2018, July). Enhancing cybersecurity skills by creating serious games. In *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education* (pp. 194-199).

Taylor-Jackson, J., McAlaney, J., Foster, J. L., Bello, A., Maurushat, A., & Dale, J. (2020). Incorporating psychology into cyber security education: a pedagogical approach. In *Financial Cryptography and Data Security: FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers 24* (pp. 207-217). Springer International Publishing.

Triantafyllou, S., & Georgiadis, C. K. (2022). Gamification of MOOCs and security awareness in corporate training.

Twitchell, D. P. (2007). SecurityCom: a multi-player game for researching and teaching information security teams. *Journal of Digital Forensics, Security and Law*, *2*(4), 1.

Ungerer, L. M. (2016). Digital curation as a core competency in current learning and literacy: A higher education perspective. *The International Review of Research in Open and Distributed Learning*, *17*(5).

Vargas, J. A., García-Mundo, L., Genero, M., & Piattini, M. (2014, May). A systematic mapping study on serious game quality. In *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering* (pp. 1-10).

Vermunt, J. D., & Verloop, N. (1999). Congruence and friction between learning and teaching. *Learning and instruction*, *9*(3), 257-280.

Wang, C. J., Liu, W. C., Kee, Y. H., & Chian, L. K. (2019). Competence, autonomy, and relatedness in the classroom: understanding students’ motivational processes using the self-determination theory. *Heliyon*, *5*(7).

Wangen, G. (2017). Information security risk assessment: a method comparison. *Computer*, *50*(4), 52-61.

Wouters, P., Van Nimwegen, C., Van Oostendorp, H., & Van Der Spek, E. D. (2013). A meta-analysis of the cognitive and motivational effects of serious games. *Journal of educational psychology*, *105*(2), 249.

Yıldız, G., Yıldırım, A., Akça, B. A., Kök, A., Özer, A., & Karataş, S. (2020). Research trends in mobile learning. *International Review of Research in Open and Distributed Learning*, *21*(3), 175-196.

Zafeiropoulou, M., Volioti, C., Keramopoulos, E., & Sapounidis, T. (2021). Developing physics experiments using augmented reality game-based learning approach: A pilot study in primary school. *Computers*, *10*(10), 126.

Zeng, J., Parks, S., & Shang, J. (2020). To learn scientifically, effectively, and enjoyably: A review of educational games. *Human Behavior and Emerging Technologies*, *2*(2), 186-195.

Zhao, X., Xie, H., Roberts, A., & Sbaffi, L. (2024, April). Promoting Academic Integrity Through Gamification: Testing the Effectiveness of a 3D Immersive Video Game. In *International Conference on Information* (pp. 65-76). Cham: Springer Nature Switzerland.