applied sciences

MDPI

Article

Assessing the Effects of Gamification on Enhancing Information Security Awareness Knowledge

Tienhua Wu [1], Kuang-You Tien [2], Wei-Chih Hsu [3] and Fu-Hsiang Wen [1,4,*]

1 Department of Management, Air Force Institute of Technology, Kaohsiung 82047, Taiwan; 9428901@nkust.edu.tw
2 Center for General Education, Air Force Institute of Technology, Kaohsiung 82047, Taiwan; s108106905@ncnu.edu.tw
3 Department of Computer and Communication Engineering, National Kaohsiung University of Science and Technology, Kaohsiung 81164, Taiwan; weichih@nkust.edu.tw
4 PhD Program in Engineering Science and Technology College of Engineering, National Kaohsiung University of Science and Technology, Kaohsiung 81164, Taiwan
* Correspondence: 0615905@nkust.edu.tw

Abstract: Information security awareness (ISA) has become a vital issue, as security breaches often attributed to humans lead to losses for individuals and organizations. Information security (IS) education may be an effective strategy to improve students' ISA; however, studies associated with the relationships between teaching effects and information security learning are few. This study adopted gamification practice and examined its effect on students' ISA knowledge enhancement, attitude and intention of security compliance, and willingness for continuous IS education. This study also examined the gender difference in a gamified learning system. One hundred ten undergraduates participated in a quasi-experimental study. The results indicated that students within a gamified class performed better than students within a lecture-based instructional group. We found significant gamification effects on the three security focus areas of password management, Internet use, and information handling. Gamification did not significantly impact the attitude and intention of participants' security compliance and students' willingness for continuous IS learning. Gender difference in the effect of gamification on ISA knowledge enhancement was not observed as well. The research provides theoretical and practical contributions by incorporating gamification into IS learning and suggests gamification as an effective means to enhance students' knowledge acquisition in an engaging, timely, economical, and repeated manner.

Keywords: information security awareness (ISA); gamification; ISA knowledge; attitude; intention; security compliance

Citation: Wu, T.; Tien, K.-Y.; Hsu, W.-C.; Wen, F.-H. Assessing the Effects of Gamification on Enhancing Information Security Awareness Knowledge. *Appl. Sci.* **2021**, *11*, 9266. https://doi.org/10.3390/app11199266

Academic Editors: Wen-Hsiang Hsieh, Jia-Shing Sheu, Minvydas Ragulskis and Arcangelo Castiglione

Received: 2 August 2021
Accepted: 24 September 2021
Published: 8 October 2021

1. Introduction

Information security awareness (ISA) has become a vital issue for scholars and practitioners given an individual's increased risky behaviors along with a growth of the size of networks and Internet applications [1,2]. Information security (IS) has also been a significant concern to educators [3]. According to an EDUCAUSE review [4], IS refers to developing a holistic, agile approach to reduce institutional exposure to IS risks and is the top information technology (IT) issue of foundations for student success. Moreover, students and the use of computers and the Internet have become inseparable, suggesting students are at a higher risk of exposing themselves to IS threats such as hacking, malware, and viruses [5,6]. IS breaches can lead to losses and damages at the individual and organizational levels. Thus, equipping students with adequate ISA knowledge and concepts is essential for future professional life and societies [3,7–9].

However, teaching ISA knowledge is challenging. First, security includes a wide range of subjects and modules, such that IS curricula are not being adequately addressed

in undergraduate programs [3]. Second, information risk profiles continue to change, such that IS training and education provide relevant and timely knowledge [2,9]. Third, budget and resource constraints are the main barriers to ISA programs in universities [7]. Lastly, given students' learning behaviors and limited experience, the previous literature suggested varying teaching methods, such as media richness systems [2], e-learning approach [10], virtual training [7], hands-on learning [6], or gamification training [11], may potentially benefit students to improve ISA. Hence, effective IS training and education rely on content materials and learning methods to achieve desired outcomes in the educational, economic, and social fields [3].

Despite the difficulties, scholars [5,10,12] emphasized the urgent need for IS training and education because human factors significantly predict employees' and students' security beliefs and behaviors. Vroom and Von Solms [13] noted that according to the 2001 Information Security Industry survey, 48 percent of the security breaches were accidental and may result from negligence or ignorance of an organization's IS policies. The technical side of the organization cannot achieve security objectives; educating the security attitude of employees [5] or changing a more IS conscious organizational culture [13–15] or encouraging end-user involvement in IS compliance [14,15] are also vital to ensure adequate security. IS education thus becomes an effective strategy that motives students' security attitude and likely prevents students from being the weakest link in a security chain [16]. It is thus essential to offer adequate IS education for students to understand IS knowledge, train security best practices, and repeat training regularly to increase their awareness and commit to security compliance [6,7].

Accordingly, this study incorporated a novel educational practice, gamification, into IS education and examined its effect on enhancing students' ISA knowledge and students' attitudes toward and intentions to comply with security policies. Given an influential role of gender in students' learning and security behaviors [17–19], this study also explored gender differences in IS learning under a gamified education setting. The following questions were investigated:

RQ1: Does gamification practice enhance students' overall ISA knowledge performance or specific security subjects?

RQ2: Does gamification practice influence students' attitude and intention to comply with security policies and students' willingness to learn IS subject?

RQ3: Does gender moderate the effect of gamification practice on students' ISA knowledge enhancement?

This study continues to review the relevant literature on information security awareness and gamification. This study then outlines the methodology of participants and procedure and the results of the data analysis. Finally, this study discusses the findings from the empirical evaluation and provides implications and suggestions for future research.

2. Literature Review

2.1. Information Security Awareness Knowledge

Parsons et al. [1] suggested that information security awareness (ISA) underpins the three aspects: knowledge, attitude, and behavior. If an employee is with adequate ISA, he/she would be knowledgeable about safe IS behaviors, committed to, and behave following best practices. In the context of health information security awareness (HISA), Park et al. [16] integrated the three concepts into HISA, namely, general ISA, health information security regulation awareness, and punishment severity awareness. Given our research aims, ISA knowledge in this study is defined as the extent to which students knowledge about the importance and implications of safe information security behaviors outlined in written policies, rules, and guidelines [1,16].

This study employed the Human Aspects of Information Security Questionnaire (HAIS-Q) developed by Parsons et al. [1] to measure students' ISA knowledge. The HAIS-Q consists of a wide range of IS subjects: password management, email use, Internet use, social media use, mobile devices, information handling, and incident reporting. Parsons et al. [1] showed that the HAIS-Q may provide a complete understanding of cybersecurity vulnerabilities caused by human behavior. The IS focuses of the HAIS-Q are primarily aligned with IS education topics suggested by Futcher et al. [3] and with students' perceived threats domains identified by Farooq et al. [20]. Empirically, the HAIS-Q measurement was utilized to examine the relationship between individual differences and ISA [19] and explain undergraduates' problematic information security behaviors [21]. Consistent with the prior works, this study assumes that the HAIS-Q is a robust measurement to assess students' ISA knowledge as a significant predictor of security behaviors.

Many security breaches are attributed to human errors [13,18,22]. Literature suggested that human's attitude and behaviors often exhibit weaknesses or vulnerabilities that likely lead to opportunistic attacks [7,10,23], particularly in those who has insufficient technical experience or are not aware of opportunistic attacks such as social engineering [12]. For example, Rezgui and Marks [5] surveyed university staff and found that lack of IS awareness may lead to non-technical threats such as user errors, software failure, social engineering problems, and data leakage problems. Human factors such as personal norms, self-control [16], perception of privacy and responsibility [14], and mindful awareness [21] were negatively associated with deviant behaviors. Furthermore, scholars [5,13] stressed that considering human behaviors is beneficial in improving an organization's security culture, thereby reducing violations against security policies. Overall, along with advancements in the Internet and technological devices, the role of humans has increasingly expanded in addressing IS [23]. Moreover, human factors are intrinsic, and organization leaders often have limited influence on them [14]. Hence, in addition to rewards and sanctions, IS research highly recommended that ISA training and education is an essential part of defensive security policies to motivate students toward awareness of security policies [3,5,10,15,16].

In the context of IS training and education research, certain studies mainly focused on normative suggestions [3,9]; several scholars examined the individual factors and characteristics influencing students' security beliefs and behaviors [6,14,16], whereas certain research provided empirical results concerning students' status of ISA knowledge [7,10]. Recently, Heid et al. [11] presented an approach of security training gamification to raise employees' awareness and keep their engagement in regular practicing. Ros et al. [8] developed a cybersecurity educational game and validated its positive correlation to learning achievement. However, few studies explore the teaching effects on learners' IS performance and their compliance beliefs and behaviors from an educational perspective. This study aims to understand whether a gamified educational system influence students' ISA knowledge enhancement, attitude toward, and intention to security compliance.

2.2. Gamification and Learning

Gamification defines as integrating game elements into non-game environments [24]. Unlike a digital game, gamification practice integrates varying game mechanics, such as points, levels, leaderboards, and badges, into learning contexts or platforms to make learning more fun and motivating [25–27]. Hamari et al. [28] noted that serious games likely focus on learning content, while the objective of gamification mainly achieves learner's engagement and motivation. Martí-Parreño et al. [27] suggested that serious games aim to learn while having fun; gamification can be used to achieve performance and social dynamics and interactions. However, differentiating between gamification and serious games is complex [29]. Thus, given our research design, this study used 'gamification' as a term that encompasses a digital game and gamification elements simultaneously utilized in our study.

The most popular game mechanics are points, badges, levels, and leaderboards [24,28]. According to Buckley and Doyle [30], points are a numeric record of players' performance to date; badges are the visual representation of achievement; levels related to difficulty moderated based on player expertise, and leaderboards are used to allow the direct comparison of players' expertise. The purposes and uses of game elements vary. Points provide feedback; levels and leaderboards are utilized to set up clear goals [31]. Badges reward users' challenge and participation achievements and levels are employed to differentiate games, playing, or players for increasing challenges [24]. Therefore, the usage of game mechanics depends on the aims of curricula or game design.

The previous studies have examined specific game elements influencing students' psychological states or meaningful learning. For example, Hamari [32] identified that badges used for goal and feedback purposes significantly increase behavioral consequences. Sailer et al. [33] noted that badges, leaderboards, and performance graphs positively affect competence need satisfaction and perceived task meaningfulness. Garcia-Iruela and Hijón-Neira [34] considered time durations of the game experience and noted that points and levels were the best valued by students in the different time durations. In contrast, Hanus and Fox [35] found that badges and leaderboards harm motivation because earning badges may become mandatory for those in the gamified class, decreasing intrinsic motivation. Garcia-Iruela and Hijón-Neira [34] identified that badges were well perceived by students in the longest experience but were the worst-related elements in the two-week experience. Consequently, despite that game mechanics may promote users' positive outcomes, considerations such as participants' commitment and characteristics [32,35], educational setting aspects such as curricula, activities, and instructors [35], or time duration of game usage [34] are emphasized for effective gamified education.

Furthermore, the effectiveness of gamification in an educational context has been previously addressed [24,28,36,37]. Gamification has been increasingly utilized to promote psychological and behavioral outcomes [26,28,33] and bridge the distinction between formal and informal learning for cognitive development [29]. The positive impacts include psychological need satisfaction such as competence, autonomy, and social relatedness [33], positive affective states [36], or performance achievement and knowledge acquisition [36,38]. In contrast, certain research provides insignificant or mixed results [26,39,40]. In sum, given meta-analysis reviews on gamification in education, Dicheva et al. [24] and Koivisto and Hamari [37] concluded that the majority of researchers confirmed that gamification could improve learning if it is well designed and used correctly.

According to Ros et al. [8], cybersecurity has emerged as a new topic in games across different disciplines. Limited research focuses on IS gamification and its impact. Recently, Heid et al. [11] demonstrated the implementation of a security training gamification in mobile security; Ros et al. [8] designed a cybersecurity game and suggested a higher correlation between playing the game and succeeding in the course. However, there are few studies associated with relationships between gamification and subjects such as IS learning [24]. Hence, this study adopted gamification practice and examined its effect on students' ISA knowledge enhancement, attitude toward, and intention to IS compliance.

3. Methodology

3.1. Participants

Participants were 110 college students in Taiwan who enrolled in a basic computer science course and showed their interest in ISA knowledge learning and games to volunteer. Among the 110 students, 52.7 percent of the subjects were males, and respondents were in the 18 to 21 age range (M = 19.51, SD = 0.687). The sample was evenly distributed in terms of demographic factors. This study used a quasi-experimental design. The students were assigned to both groups for IS learning with and without gamification mechanisms. One class (56 students) was assigned to learn ISA knowledge by a digital game within a gamified classroom (game-based group). The other class, including 54 students, learned within a lecture-based instructional classroom (lecture-based group). The subjects among

the two groups showed no statistical differences in their IS learning background ($t = 1.421$, $p > 0.05$), nor in their previous video game experiences ($t = 0.215$, $p > 0.05$) and nor in their usage hours of the Internet per week ($t = -1.292$, $p > 0.05$).

3.2. Procedure

This study adopted a quasi-experimental design with pretests and posttests to evaluate all students who participated in this study. During the pre-experiment session, all subjects were informed of the purposes and procedures of this experiment. Before the experiment, the two groups of students first had four weeks of classes about introduction knowledge to computer science that enables the students to have the fundamental computer concepts and basic skills to operate computers. However, they all did not know IS subjects before the experiment.

Next, this study took a week to pretest the HAIS-Q developed by Parsons et al. [1]. The HAIS-Q has statements about students' ISA knowledge of how to use a computer for work/schools and consists of the seven areas, including password management, email use, Internet use, social media use, mobile devices, information handling, and incident reporting. This questionnaire assessed students' general knowledge about ISA rather than IS technical or theoretical concepts. The two groups had an equivalent evaluation of IS learning before and after the treatment.

Third, the experiment was conducted as a 4-week experiment, and the IS learning materials were delivered through gamification and lecturing methods. The ISA knowledge topics included in the game-based and lecture-based classes are shown in Table 1. In a game-based group, the teacher introduced the *PaGamO* website and IS digital game application, guided students to register and browse the *PaGamO* website, and explained its basic instructions to ensure that students know game mechanisms and rules. During the experiment period, participants were required to individually sign into the website at least three times a week, and each was fifty-minute long. Students were asked to complete their gaming tasks. Thus, except for the game design provided by the current IS learning game, we integrated levels and leaderboard gamification mechanics into the class to promote individual students' engagement and achievement. In a lecture-based group, the teacher delivered lectures regarding ISA knowledge, provided discussion panels or teaching activities in class that help students enhance their understanding, and had quizzes every week to confirm students' conceptual understanding. Similarly, the instructor in a lecture-based group attempted to increase students' performance and motive students' learning. The teacher used teaching strategies such as an interactive or cooperative method to promote students' engagement and provided real-time feedback to their questions and discussion.

Last, the participants in both groups took the posttests of the HAIS-Q questionnaire after the four-week experimental learning. The students were also asked to complete the questionnaire regarding their attitude toward security compliance, their intention to avoid potential security breaches, and their willingness to continuously gain IS education.

3.3. Measures

This study employed the questionnaire of the knowledge section of the HAIS-Q [1] to investigate whether gamification practice enhances students' ISA knowledge. The HAIS-Q questionnaire used 21 items to assess students' ISA general knowledge of the seven areas: password management, email use, Internet use, social media use, mobile devices, information handling, and incident reporting. As mentioned earlier, the HAIS-Q was appropriate to measure students' performance because of its consistency with IS education topics [3] and students' perceived threats domains [20]. Table 1 shows the connection between ISA knowledge topics and the areas of the HAIS-Q. Students' attitudes toward and intentions to comply with the IS policies originated from the study [22]. Students' attitude toward security compliance was related to the degree to which the performance of the compliance behavior is positively valued [22]. The construct of intention was used

to assess an individual's intention to protect the information and technology resources of the organization from potential security breaches [22]. All variables were measured with multiple items on seven-point Likert scales, ranging from *strongly disagree (coded as 1)* to *strongly agree (coded as 7)*, and each of the study variables consisted of three to four items. This study also surveyed whether students are or are not willing to gain continuous IS education. All questionnaire items are presented in Appendix A.

Table 1. ISA knowledge topics and the HAIS-Q.

Week	ISA Areas	Topics	HAIS-Q
Week 1	IS principles and policies	• Cybersecurity fundamentals • Information security management • Compliance and legal issues	• Password management • Email use • Internet use • Social media use • Information handling • Incident reporting
Week 2	Cybersecurity of the network	• Operating system security • Software security • Network security	• Password management • Email use • Internet use
Week 3	Attack methods and basic defense against attacks	• Social engineering • Attacks and defenses • Web security	• Email use • Internet use • Social media use • Information handling
Week 4	Security management of mobile devices, USB, and database	• Database security • Information assurance	• Password management • Internet use • Social media use • Mobile devices • Information handling

3.4. Information Security learning Game System

A free web-based IS digital game (IS learning game) provided by *PaGamO* was utilized in this study to help students learn ISA knowledge. *PaGamO*, developed by Taiwanese Company *BoniO Inc.*, is the world's first online gamification learning platform. This platform offers multiple subjects and programs, ranging from elementary school to adult education and training, and more than 1.5 million global users participate in individual or collaborative online gamification learning. The IS learning game system offers an updated cloud-based, hierarchical user interface that allows students to use computers or mobile devices and intuitively assess ISA knowledge learning materials under a gamification mechanism. Such benefits and affordance may reduce the bias concerning technical difficulties that affected students' learning performance [41]. Furthermore, Cheung and Ng [42] empirically identified that the scores of the *PaGamO* educational game related to examination scores. Accordingly, an IS learning game of *PaGamO* is a suitable tool for examining the gamification effects on students' ISA knowledge enhancement.

The IS learning game system has three primary databases: a user's profile, IS knowledge materials, and gamification mechanisms. A user's profile database saves users' registration information and automatically records participants' learning performance status and behaviors in a game. An IS knowledge and materials database stores the IS learning materials in terms of awareness, technical, and management categories provided by the *PaGamO* course designers. Given the time limitation and ISA knowledge topics implemented in this study, this study mainly focused on the awareness knowledge category because the current IS learning game includes the learning materials of the ISA topics shown in Table 1. The knowledge materials database also allows teachers to build specific learning tasks, but the instructor did not use this function in the current study. The gamification mechanisms database includes the game dynamics and mechanics. Figure 1 shows the architecture of the IS learning game system, and Figure 2 displays a front page screenshot of IS learning game.

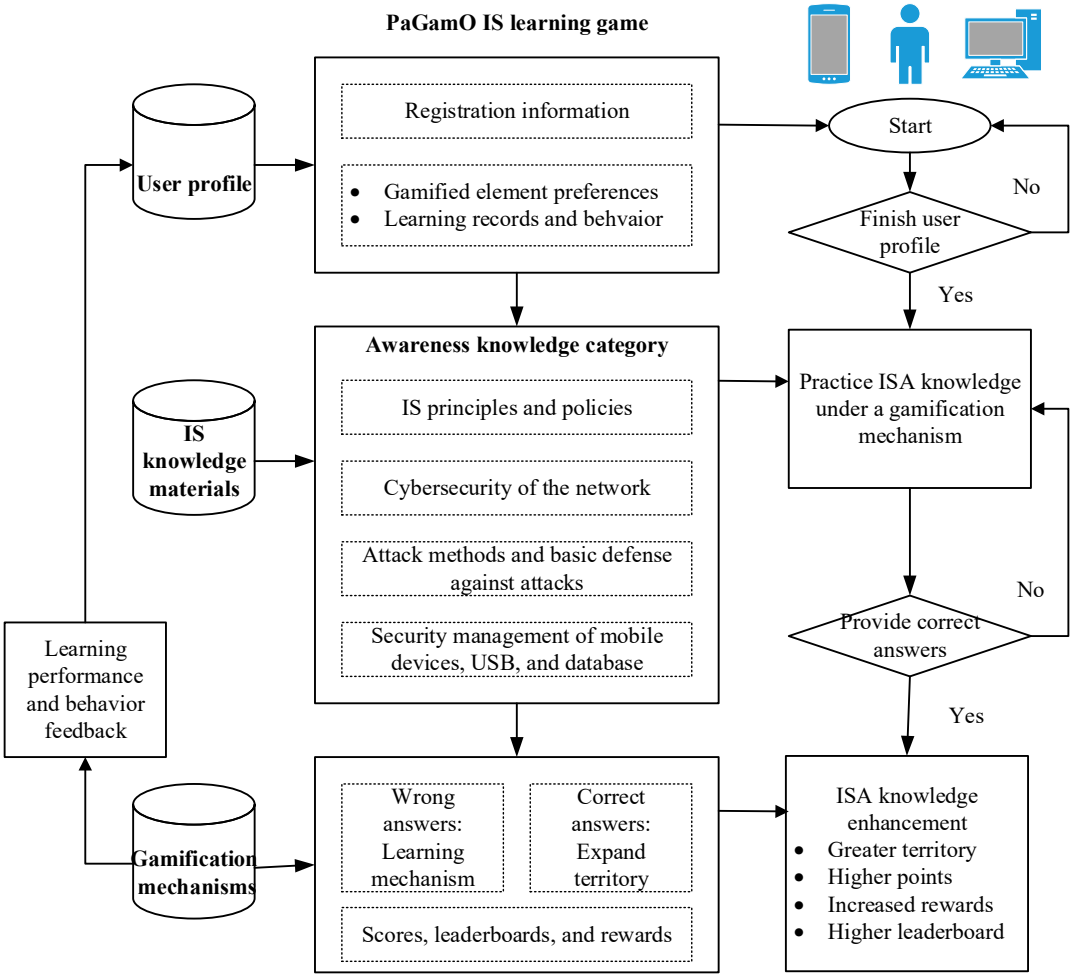


Figure 1. IS (Information Security) learning game architecture.

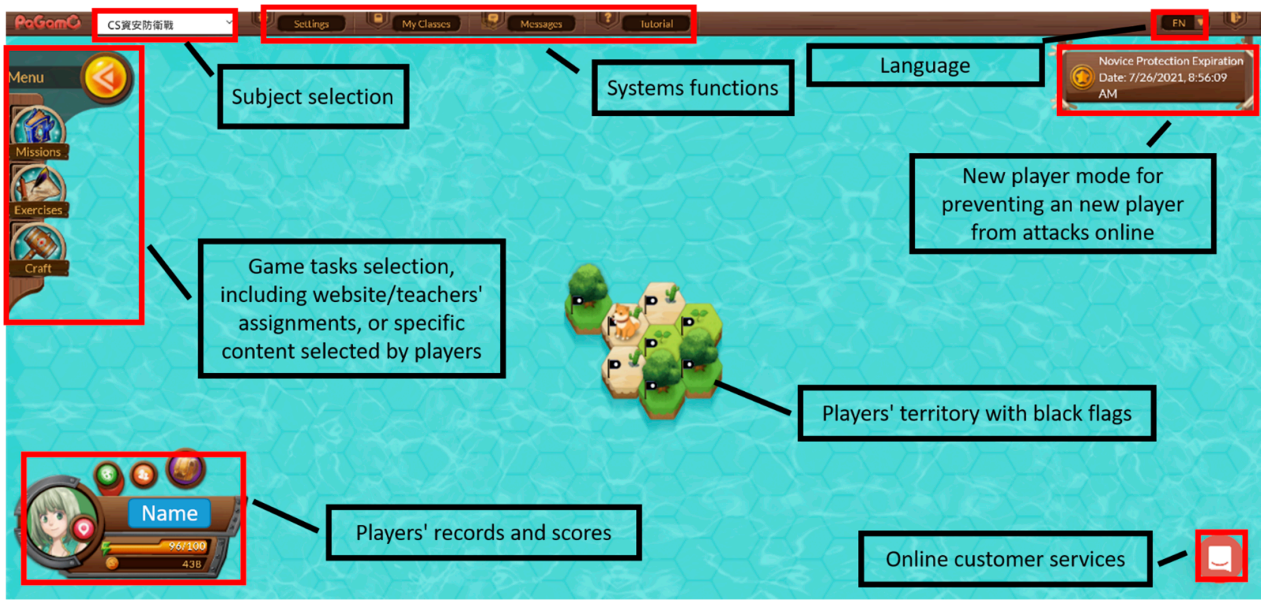
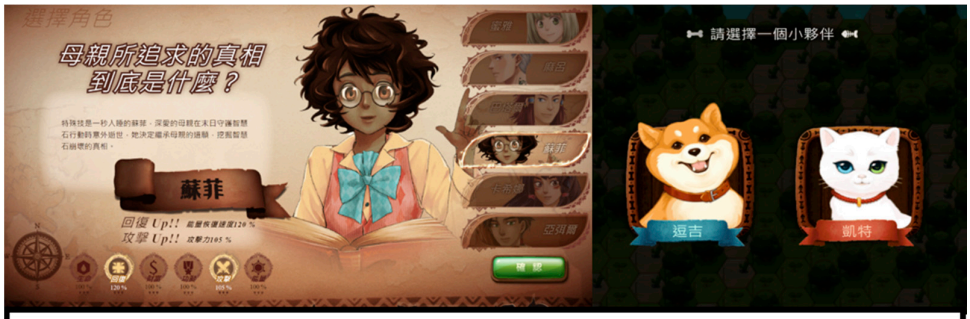
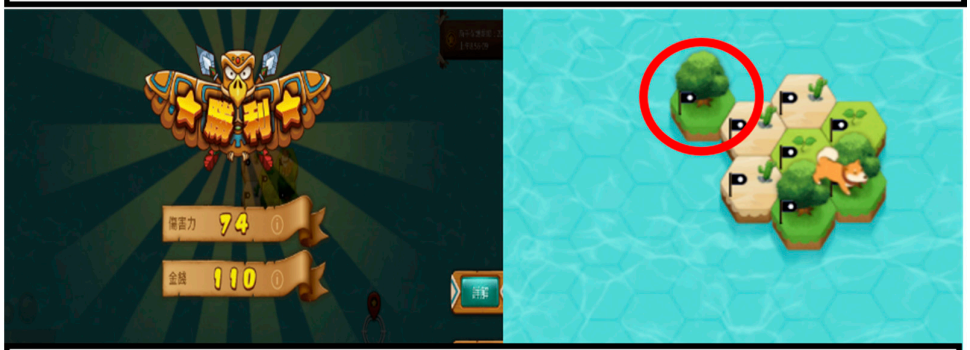


Figure 2. Frontpage screenshot of IS learning game for registration. Source: PaGamO website. Note: Non-English words in the Figure 2 represent game subject selection of 'Information security game task' in Chinese.



Step 1: Select game avatars with varying skills and tools

Step 2: Expand territory by answering multiple choice questions associated with ISA knowledge



Step 3: Expand territory successfully by providing correct answers

Step 3: Provide learning mechanisms when wrong answers occur

Figure 3. *Cont.*

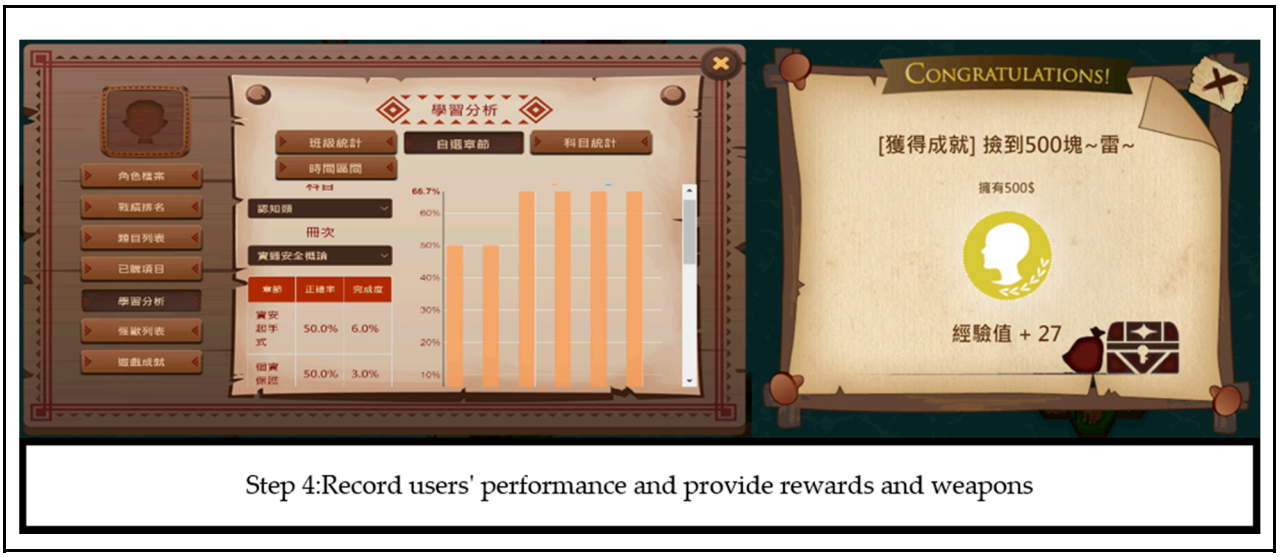


Figure 3. IS learning game interface and procedure. Source: PaGamO website. Note: Non-English words in the screen of the step 1 show the brief descriptions of game task and introduction to the skills and tools of game avatars in Chinese. The screen of the step 2 represents the ISA multiple question and answers concerning firewall issue when users selected a specific territory that they aimed to challenge. The two screens of the step 3 are the expanded territory when users submitted the correct answers and a learning mechanism of correct answer and explanations concerning virus issue when users did not challenge successfully. The screen of the step 4 relates to a user's achievement information in Chinese that are leaderboard, points, weapons, and rewards gained when completed the game tasks.

Figure 3 shows the IS learning game interface and procedure. First, students needed to register on the *PaGamO* website and selected avatars for games individually or collaboratively (Step 1 of Figure 3). A user's profile database also automatically recorded their learning performance status and learning behaviors in the games. Next, students practiced ISA knowledge under gamification mechanisms. Participants selected gaming tasks from the three sources of website, teachers, or specific topics for a repeated practice purpose, responded to questions correctly to gain scores (i.e., expand users' territory), or learned from website learning mechanism for advancement when incorrect answers were given (Steps 2 and 3 of Figure 3). Last, this IS learning game adopts several gamification design elements such as points, leaderboards, rewards, tools, or weapons. Once participants finished their tasks successfully, their territory became greater; their experience points became higher; their weapons or tools as bonuses increased; their abilities on the leaderboards also showed stronger (Step 4 of Figure 3).

4. Results

4.1. Assessment of Measurement Validation

The data was analyzed in SPSS 20 software. Cronbach's alpha (α) was used to assess measurement reliability. Table 2 provides descriptive data, correlations, and Cronbach's alpha of the study variables. The values for Cronbach's alpha of most study variables were above the required value of 0.7. Three variables' α values were lower than 0.7 but higher than or equaled to 0.6, suggesting the reliability of study variables was acceptable [43]. The correlations between focus areas of ISA, attitude, and intention ranged from 0.39 to higher to 0.89, and all correlations were significant ($p < 0.01$).

4.2. Effects on Information Security Awareness Knowledge

Although the teachers differed across the classes, our pre-experiment assessment regarding ISA knowledge showed no significant differences ($t = 0.397$, $p > 0.05$). It is fair to assume that the two groups started with a similar level of knowledge, suggesting a further analysis was acceptable. This study employed an independent samples t test to examine

the effect of gamification on students' ISA knowledge enhancement in terms of overall and specific focus areas of ISA. Table 3 shows the descriptive statistics and results of samples *t* test, effect sizes, and observed power among game-based and lecture-based groups.

Table 2. Descriptive results, correlations, and Cronbach's alpha of the variables.

	M	SD	α	1	2	3	4	5	6	7	8
1. PM	17.69	2.50	0.61								
2. EU	17.75	2.65	0.68	0.56							
3. IU	16.53	3.17	0.80	0.64	0.51						
4. SMU	16.87	3.10	0.60	0.46	0.41	0.59					
5. MD	17.19	2.75	0.70	0.57	0.48	0.58	0.67				
6. IH	18.13	2.83	0.79	0.60	0.53	0.55	0.56	0.73			
7. IR	17.38	3.07	0.73	0.55	0.46	0.48	0.50	0.67	0.65		
8. ATT	25.41	3.48	0.94	0.44	0.44	0.46	0.39	0.52	0.63	0.62	
9. IN	19.33	2.49	0.96	0.47	0.45	0.48	0.41	0.62	0.66	0.62	0.89

Note: N = 110. PM: password management; EU: email use; IU: Internet use; SMU: social media use; MD: mobile devices; IH: information handling; IR: incident reporting; ATT: attitude; IN: intention. All correlations are significant ($p < 0.01$).

Table 3. Results of *t* test on ISA knowledge.

ISA Focus Areas	Groups	Mean	SD	*t* Test	*p* Value	η^2	Observed Power
Overall	Game-based Lecture-based	124.54 118.43	13.32 17.66	2.04	0.04 *	0.04	0.53
Password management	Game-based Lecture-based	18,25 17.11	1.92 2.90	2.42	0.02 *	0.05	0.68
Email use	Game-based Lecture-based	18.07 17.41	2.48 2.79	1.32	0.19	0.02	0.26
Internet use	Game-based Lecture-based	17.38 15.65	2.53 3.54	2.94	0.00 **	0.08	0.83
Social media use	Game-based Lecture-based	17.18 16.56	2.73 3.45	1.05	0.30	0.01	0.18
Mobile devices	Game-based Lecture-based	17.43 16.94	2.61 2.89	0.92	0.36	0.01	0.15
Information handling	Game-based Lecture-based	18.79 17.44	2.49 3.01	2.55	0.01 *	0.06	0.72
Incident reporting	Game-based Lecture-based	17.45 17.31	3.16 3.01	0.22	0.82	0.05	0.06

Note: * $p < 0.05$, ** $p < 0.01$.

The results indicated that an IS learning game had a significant effect on students' overall security learning performance. Students within a gamified class performed better than that of students within a lecture-based instructional group ($t = 2.04$, $p < 0.05$, $\eta^2 = 0.04$, observed power = 0.53). In addition to overall posttest performance, a closer look at specific ISA focus areas revealed that the differences between two groups were found. The performance differences were observed in three areas of password management ($t = 2.42$, $p < 0.05$, $\eta^2 = 0.05$, observed power = 0.68), Internet use ($t = 2.94$, $p < 0.01$, $\eta^2 = 0.08$, observed power = 0.83), and information handling ($t = 2.55$, $p < 0.01$, $\eta^2 = 0.06$, observed power = 0.72).

4.3. Effects on Students' Attitudes, Intentions, and Continuous Information Security Learning

This study further investigated the effects of gamified teaching methods on students' attitudes toward and intentions to IS compliance by an independent samples *t* test. Unex-

pectedly, neither a significant gamification effect on students' attitude variable (t = 0.05, $p > 0.05$) nor a significant gamification effect on students' intention variable ($t = -0.27$, $p > 0.05$) emerged. The analysis findings of students' attitudes and intentions are presented in Table 4. In addition, this study assessed students' willingness to continuously gain IS education after the experiment. The results indicated that 47 students of a game-based group (83.9%) and 50 students of a lecture-based group (92.6%) showed they were willing to learn IS subject after this study. Participants engaged in a game-based group did not differ significantly from participants in a lecture-based group on their willingness for continuous IS learning (t = 1.42, $p > 0.05$).

Table 4. Results of t test on attitude and intention.

Dependent Measure	Groups	Mean	SD	t Test	p Value	η^2	Observed Power
Attitude	Game-based	25.32	3.36	0.05	0.96	0.00	0.06
	Lecture-based	25.50	3.62				
Intention	Game-based	19.34	2.38	−0.27	0.79	0.00	0.05
	Lecture-based	19.31	2.61				

4.4. Effects of Gamification and Gender

Table 5 shows the number of participants among the two groups by gender and the means and standard deviations for students' overall posttest performance of the HAIS-Q. A two-way ANOVA revealed that groups generate gamification of significantly higher ISA knowledge enhancement (F = 3.7, $p \leq 0.05$, η^2 = 0.03). In contrast to group results, neither a significant main effect for gender on gamified learning of ISA knowledge (F = 0.01, $p > 0.05$) nor a significant interaction between groups and gender was observed (F = 1.81, $p > 0.05$).

Table 5. Results of descriptive data based on groups and gender.

	Game-based		Lecture-based	
ISA knowledge	Males (N = 24)	Females (N = 32)	Males (N = 34)	Females (N = 20)
	Mean (SD)	Mean (SD)	Mean (SD)	Mean (SD)
Overall	126.71 (14.11)	122.91 (12.68)	116.79 (17.84)	121.20 (17.46)

Note: The numbers in the parentheses are standard deviations.

5. Discussions

The first research question (*RQ1*) aimed to identify whether gamification practice enhances students' overall and the specific areas of Information security awareness (ISA) knowledge. The current study's findings suggested that gamification effectively supports learning achievement in information security awareness knowledge. Notably, a gamified education system significantly impacts the three specific focus subjects: password management, Internet use, and information handling. *RQ2* aimed to answer whether gamification practice influences students' attitudes and intentions to comply. On the contrary, neither a significant effect of gamification on students' attitudes nor IS compliance intentions. Gamification practice also did not impact students' willingness to learn continuously IS subject. The third question (*RQ3*) addressed whether gender moderates gamification practice on students' learning performance. The results revealed that the moderating effect of gender influencing the relationship between gamification and IS knowledge enhancement was not found. We discuss the findings from the empirical evaluation as follows.

First, the results indicated that the overall ISA performance of students in a gamified classroom is significantly superior to that of students in a lecture-based classroom. An IS learning digital game here provided a media richness experience that likely improves students' attention, understanding, and recall [2,11]. When users' incorrect answers were given, the online learning mechanism may offer time-efficient and continuous exercises [6,7]

and trial and error learning paths for individual learners [25]. The game elements with points, rewards, and leaderboards likely became motivators or feedbacks to encourage students' participation and recognize their efforts [25,33]. The abovementioned benefits generated from gamification may thus contribute to the meaningful learning of learners. Additionally, gamification advanced IS education in an appealing, timely, economical, and repeated manner for teachers such that practical ISA training and education can be likely achieved [3].

Next, although gamification significantly impacted the overall performance of students, we observed the significant effects enhancing three areas of ISA rather than all areas: password management, Internet use, and information handling. The explanations could be a distinct difference between students and employees in perceiving the types and probabilities of IS threats [6,10], or students' repeated exposure to certain favored security issues for increasing awareness or meeting particular demands [5]. Thus, significant effects on all ISA areas were not found. Overall, our findings suggested that a gamified IS education system can improve participants' overall ISA knowledge. A high ISA of students likely contributes to their involvement in IS compliance, controlling their accidental deviant behaviors while heightening an organization's ISA culture that students belong to in the future [2,14–16].

Third, contradictory to our expectations, this study did not find statistical differences between two groups in students' attitudes and intentions to comply with IS policies. Achieving awareness knowledge by gamification is an essential outcome of this study but may not be adequate for participants to be confident in IS compliance. This study was consistent with the findings of Hsu and Wang [39] that gamification significantly impacts knowledge achievement rather than attitude and intention. The prior literature demonstrated that factors, such as students' self-efficacy regarding response and ability [6,7], personal norms such as moral commitment [16] or voluntary behaviors [6], or relaxed perception with limited security knowledge [7] may influence individuals' attitudes and intentions. Furthermore, learners with a conscientious personality or strong self-awareness likely prevent faults or opportunistic attacks [7,21,22]. Hence, our results implied that gamification provides an effective learning environment for knowledge enhancement but is insufficient to lead to psychological and behavioral outcomes, likely achieved by adding other education settings in gamification [38].

Fourth, the results showed no statistical difference in participants' willingness to learn IS subjects after the experiment. Similar to attitudes and intentions, gamification practice has limited impacts on outcomes such as individuals' willingness for continuous learning. Furthermore, correlations among ISA knowledge and attitude and intention were significant (see Table 2), and the mean values of students' attitudes and intentions among the two groups were higher and similar (see Table 4), implying that IS education itself may generate potential benefits for students' compliance attitudes and intentions without gamification. These results remain to be further studied in the future. The literature suggested varying considerations when addressing the effectiveness of gamification. For example, Wu et al. [44] stressed learning theories of behaviorism, cognitivism, humanism, and constructivism in game-based learning. Martí-Parreño et al. [27] suggested that potential moderators such as personality traits or game-related behaviors seem to be missed in current literature. Ros et al. [8] also noted that the design of an educational game is more than software development to achieve the expected educational goals, results, and experience. Consequently, incorporating the factors above may advance the knowledge to the influence of gamification in changing students' perception, attitude, or intention.

Fifth, considering gender factors in gamification learning contexts, differences were observed neither in gender influence nor in the interaction between gamification and gender. Unexpectedly, our results were not consistent with previous research on gender differences in ISA scores [19], self-reported security behaviors [18], or levels of ISA and abilities in dealing with security issues [17]. Both male and female students may be net-generations, and gamification and the Internet are an inseparable, essential part of their lives. Subjects' previous experiences with video games are also similar. Therefore, gender

may not be sufficient to lead to individual differences in the achievement effects. Future studies may incorporate various pedagogies in gamified IS learning to investigate gender differences.

Lastly, in addition to contributing to ISA education literature, this study also added new knowledge to research regarding gamification and learning. Consistent with the previous studies [36,38,39], this study confirmed that applying gamification to learning contexts generates encouraging outcomes related to knowledge acquisition and achievement. Specifically, the results indicated that gamification provides possible solutions to the current IS teaching challenges, for example, changing security threats and subjects [2,3], limited budgets and resources [7], or effective IS teaching contexts [2,7,10], suggesting the feasibility and efficacy of gamified IS courses. Moreover, expanding on the existing literature, this study integrated gamification into IS subject that is scarcely addressed [24] and provided empirical evidence that gamification implementations facilitated the security learning effectiveness. However, our findings did not find any positive psychological outcomes in terms of attitude and intention. The primary benefit of gamification may be a novelty effect in which the results of gamification may not be long-term [28,39,40]. As mentioned earlier, IS training should be regular [5], and attitude toward compliance can be traced back to cognitive beliefs consisting of various favorable and unfavorable consequences [22]. Therefore, given a relatively short experimental period in this study, gamification unlikely becomes an effective tool for sustainable attitude and intention changes.

6. Conclusions and Suggestions

This study investigated whether using an IS learning digital game and game mechanics simultaneously in a classroom can enhance students' information security awareness knowledge. This study further examined the effects of gamification on students' attitudes toward and intentions to IS compliance, willingness for IS continuous education, and gender differences in a gamified IS learning system. The results indicated that participants within a gamified classroom performed superiorly in ISA knowledge acquisition than those within a lecture-based instructional classroom. The findings revealed that gamification can positively influence students' three specific IS areas: password management, Internet use, and information handling. Contrary to our expectations, gamification did not significantly impact student's security attitudes and intentions, and the influence of gender differences on the effects of gamification was not observed.

This study contributed to the literature regarding both gamification and IS learning. These results suggested that gamification enhances students' knowledge acquisition in an appealing, timely, economical, and repeated manner. Such selected gamification mechanics and dynamics foster students' IS learning. This study thus enriches the literature by addressing the feasibility and efficacy of incorporating gamification in security education that has received less than adequate attention [8,20,24]. This study contributes to observing the ways and outcomes of security education that may have a deterrent influence on students' deviant behavior in their future careers [12,16] and further lead to a security policy compliance culture in an organization [14,15].

This study also had practical implications. Using digital technology in the classroom is a trend in education. This study provided a free gamification learning platform as an alternative that can make boring IS tasks and materials more engaging and enjoyable [8,11] and make IS learning more feasible and regular [2,7,9]. Despite that, these results suggested that the game mechanics such as points and leaderboard can be applied in a traditional classroom, raising the learning interests in boring, challenging subjects [24].

This study had several limitations and future directions. First, the experiment was conducted over a short period. The time variable could become an essential factor influencing the effectiveness of gamification [34]. Future studies can utilize longitudinal design to provide evidence on whether using game mechanics may be effective over the long run in improving students' IS learning and compliance intention [28,39,40]. Further,

while this study mainly used ISA knowledge to measure participants' performance, many varying cognitive–behavioral factors [37], individual learning characteristics [25,30], educational setting factors such as curricula, pedagogies, or instructors [35,38], or learners' game learning experience and behavior [44,45] were neglected. A future study may benefit from incorporating these considerations that provide additional insights into how game mechanics support deeper learning and strengthen students' compliance beliefs and behaviors. Third, this study used a quasi-experiment method and only game and lecturing instructional approaches that could not provide sufficient evidence. The researchers may consider a laboratory experiment, other teaching methods, or new algorithms for learners' behavior [45] to gain a richer understanding of gamification in education. Lastly, although gender difference was not observed in the current study, future studies focusing on gender are recommended, as age and gender have produced mixed results on the HAIS-Q [1]. In the context of IS education, gender-specific gamification practices, pedagogies, and content materials may offer the potential to increase awareness, improve compliance attitude, and further commit to security behaviors [17].

Author Contributions: Conceptualization, T.W.; project administration and supervision, T.W. and W.-C.H.; methodology, K.-Y.T.; investigation, K.-Y.T. and F.-H.W.; formal analysis, T.W. and F.-H.W.; writing–original draft, T.W. and F.-H.W.; writing-review and editing, T.W. and K.-Y.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Ministry of Science & Technology, Taiwan. MOST 109-2511-H-344-001; MOST 110-2511-H-344-001-MY3.

Institutional Review Board Statement: Ethical review and approval were waived for this study, due to the following conditions issued by the Governance Framework for Human Research Ethics at National Cheng Kung University in Taiwan: (1) participants of this study are not homeless, children and adolescents, native citizens, new immigrants, pregnant women, handicappers, or psychiatric patients; (2) the likelihood of damages or discomfort derived from participating in this study is not higher than the chance of any other damages or discomfort in participants' daily life; (3) decisions to take or not to take part in this study do no influence participants' rights and benefits; (4) participants do not provide personal information; (5) the collection data is appropriately saved by researchers' institutions and used only for this study, and (6) the collection data is unrelated to any specific participant, organization, or circumstance.

Informed Consent Statement: Informed consent statement was obtained from all subjects involved in the study.

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

Appendix A

Questionnaire

Variables	Indicators
Password management	1. It is acceptable to use my social media passwords on my work accounts. 2. I am allowed to share my work passwords with colleagues. 3. A mixture of letters, numbers, and symbols is necessary for work passwords.
Email use	1. I am allowed to click on any links in emails from people I know. 2. I am not permitted to click on a link in an email from an unknown sender. 3. I am allowed to open email attachments from unknown senders.
Internet use	1. I am allowed to download any files onto my work computer if they help me to do my job. 2. While I am at work, I should not access certain websites. 3. I am allowed to enter any information on any website if it helps me do my job.
Social media use	1. I must periodically review the privacy settings on my social media accounts. 2. I cannot be fired for something I post on social media. 3. I can post what I want about work on social media.

Variables	Indicators
Mobile devices	1. When working in a public place, I have to keep my laptop with me at all times. 2. I am allowed to send sensitive work files via a public Wi-Fi network. 3. When working on a sensitive document, I must ensure that strangers cannot see my laptop screen.
Information handling	1. Sensitive print-outs can be disposed of in the same way as non-sensitive ones. 2. If I find a USB stick in a public place, I should not plug it into my work computer. 3. I am allowed to leave print-outs containing sensitive information on my desk overnight.
Incident reporting	1. If I see someone acting suspiciously in my workplace, I should report it. 2. I must not ignore poor security behavior by my colleagues. 3. It is optional to report security incidents.
Attitude	To me, complying with the requirements of the information security policies is _____. necessary 1. beneficial 2. important 3. useful
Intention	1. I intend to comply with the requirements of the information security policies of my organization in the future. 2. I intend to protect information and technology resources according to the requirements of the information security policies of my organization in the future. 3. I intend to carry out my responsibilities prescribed in the information security policies of my organization when I use information and technology in the future.
Continuous learning	After this experiment, are you willing to continuously gain IS education?

References

1. Parsons, K.; Calic, D.; Pattinson, M. The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Comput. Secur.* **2017**, *66*, 40–51. [CrossRef]
2. Shaw, R.S.; Chen, C.C.; Harris, A.L.; Huang, H.-J. The impact of information richness on information security awareness training effectiveness. *Comput. Educ.* **2009**, *52*, 92–100. [CrossRef]
3. Futcher, L.; Schroder, C.; von Solms, R. Information security education in South Africa. *Inf. Manag. Comput. Secur.* **2010**, *18*, 366–374. [CrossRef]
4. Grajek, S. Top 10 IT Issues, 2017: Foundations for student Success. 2017. Available online: http://er.educause.edu/articles/2017/1/top-10-it-issues-2017-foundations-for-student-success (accessed on 25 May 2021).
5. Rezgui, Y.; Marks, A. Information security awareness in higher education: An exploratory study. *Comput. Secur.* **2008**, *27*, 241–253. [CrossRef]
6. Yoon, C.; Hwang, J.-W.; Kim, R. Exploring factors that influence students' behaviors in information security. *J. Inf. Syst. Educ.* **2012**, *23*, 407–416.
7. Kim, E.B. Recommendations for information security awareness training for college students. *Inf. Manag. Comput. Secur.* **2014**, *22*, 115–126. [CrossRef]
8. Ros, S.; Gonzalez, S.; Robles, A.; Tobarra, L.; Caminero, A.; Cano, J. Analyzing Students' Self-Perception of Success and Learning Effectiveness Using Gamification in an Online Cybersecurity Course. *IEEE Access* **2020**, *8*, 97718–97728. [CrossRef]
9. Woodward, B.; Imboden, T.; Martin, N.L. An undergraduate information security program: More than a curriculum. *J. Inf. Syst. Educ.* **2013**, *24*, 63.
10. Stanciu, V.; Tinca, A. Students' awareness on information security between own perception and reality—An empirical study. *Account. Manag. Inf. Syst.* **2016**, *15*, 112–130.
11. Heid, K.; Heider, J.; Qasempour, K.; Darmstadt, G.K.H.F.S. Raising Security Awareness on Mobile Systems through Gamification. In Proceedings of the European Interdisciplinary Cybersecurity Conference, Rennes, France, 18 November 2020; pp. 1–6.
12. Aldawood, H.; Skinner, G. Educating and raising awareness on cyber security social engineering: A literature review. In Proceedings of the 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), Wollongong, Australia, 4–7 December 2018; pp. 62–68.
13. Vroom, C.; Von Solms, R. Towards information security behavioural compliance. *Comput. Secur.* **2004**, *23*, 191–198. [CrossRef]
14. Alshare, K.A.; Lane, P.L.; Lane, M.R. Information security policy compliance: A higher education case study. *Inf. Comput. Secur.* **2018**, *26*, 91–108. [CrossRef]
15. Amankwa, E.; Loock, M.; Kritzinger, E. Establishing information security policy compliance culture in organizations. *Inf. Comput. Secur.* **2018**, *26*, 420–436. [CrossRef]

16. Park, E.H.; Kim, J.; Park, Y.S. The role of information security learning and individual factors in disclosing patients' health information. *Comput. Secur.* **2017**, *65*, 64–76. [CrossRef]
17. Ameen, N.; Tarhini, A.; Shah, M.H.; Madichie, N.O. Employees' behavioural intention to smartphone security: A gender-based, cross-national study. *Comput. Hum. Behav.* **2020**, *104*, 106184. [CrossRef]
18. Anwar, M.; He, W.; Ash, I.; Yuan, X.; Li, L.; Xu, L. Gender difference and employees' cybersecurity behaviors. *Comput. Hum. Behav.* **2017**, *69*, 437–443. [CrossRef]
19. McCormac, A.; Zwaans, T.; Parsons, K.; Calic, D.; Butavicius, M.; Pattinson, M. Individual differences and Information Security Awareness. *Comput. Hum. Behav.* **2017**, *69*, 151–156. [CrossRef]
20. Farooq, A.; Kakakhel, S.R.U.; Virtanen, S.; Isoaho, J. A taxonomy of perceived information security and privacy threats among IT security students. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015; pp. 280–286.
21. Chen, Y.-T.; Shih, W.-L.; Lee, C.-H.; Wu, P.-L.; Tsai, C.-Y. Relationships among undergraduates' problematic information security behavior, compulsive internet use, and mindful awareness in Taiwan. *Comput. Educ.* **2021**, *164*, 104131. [CrossRef]
22. Bulgurcu, B.; Cavusoglu, H.; Benbasat, I. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Q.* **2010**, *34*, 523. [CrossRef]
23. Von Solms, R.; Van Niekerk, J. From information security to cyber security. *Comput. Secur.* **2013**, *38*, 97–102. [CrossRef]
24. Dicheva, D.; Dichev, C.; Agre, G.; Angelova, G. Gamification in education: A systematic mapping study. *J. Educ. Technol. Soc.* **2015**, *18*, 75–88.
25. Barata, G.; Gama, S.; Jorge, J.; Gonçalves, D. Studying student differentiation in gamified education: A long-term study. *Comput. Hum. Behav.* **2017**, *71*, 550–585. [CrossRef]
26. Chen, C.-M.; Li, M.-C.; Chen, T.-C. A web-based collaborative reading annotation system with gamification mechanisms to improve reading performance. *Comput. Educ.* **2020**, *144*, 103697. [CrossRef]
27. Martí-Parreño, J.; Méndez-Ibáñez, E.; Alonso-Arroyo, A. The use of gamification in education: A bibliometric and text mining analysis. *J. Comput. Assist. Learn.* **2016**, *32*, 663–676. [CrossRef]
28. Hamari, J.; Koivisto, J.; Sarsa, H. Does Gamification Work?—A Literature Review of Empirical Studies on Gamification. In Proceedings of the Annual Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 6–9 January 2014; pp. 3025–3034.
29. Adukaite, A.; van Zyl, I.; Er, Ş.; Cantoni, L. Teacher perceptions on the use of digital gamified learning in tourism education: The case of South African secondary schools. *Comput. Educ.* **2017**, *111*, 172–190.
30. Buckley, P.; Doyle, E. Individualising gamification: An investigation of the impact of learning styles and personality traits on the efficacy of gamification using a prediction market. *Comput. Educ.* **2017**, *106*, 43–55. [CrossRef]
31. Mekler, E.D.; Brühlmann, F.; Tuch, A.N.; Opwis, K. Towards understanding the effects of individual gamification elements on intrinsic motivation and performance. *Comput. Hum. Behav.* **2017**, *71*, 525–534. [CrossRef]
32. Hamari, J. Do badges increase user activity? A field experiment on the effects of gamification. *Comput. Hum. Behav.* **2017**, *71*, 469–478. [CrossRef]
33. Sailer, M.; Hense, J.U.; Mayr, S.K.; Mandl, H. How gamification motivates: An experimental study of the effects of specific game design elements on psychological need satisfaction. *Comput. Hum. Behav.* **2017**, *69*, 371–380. [CrossRef]
34. Garcia-Iruela, M.; Hijón-Neira, R. What Perception Do Students Have About the Gamification Elements? *IEEE Access* **2020**, *8*, 134386–134392. [CrossRef]
35. Hanus, M.D.; Fox, J. Assessing the effects of gamification in the classroom: A longitudinal study on intrinsic motivation, social comparison, satisfaction, effort, and academic performance. *Comput. Educ.* **2015**, *80*, 152–161. [CrossRef]
36. Acquah, E.O.; Katz, H.T. Digital game-based L2 learning outcomes for primary through high-school students: A systematic literature review. *Comput. Educ.* **2020**, *143*, 103667. [CrossRef]
37. Koivisto, J.; Hamari, J. The rise of motivational information systems: A review of gamification research. *Int. J. Inf. Manag.* **2019**, *45*, 191–210. [CrossRef]
38. Liao, C.-W.; Chen, C.-H.; Shih, S.-J. The interactivity of video and collaboration for learning achievement, intrinsic motivation, cognitive load, and behavior patterns in a digital game-based learning environment. *Comput. Educ.* **2019**, *133*, 43–55. [CrossRef]
39. Hsu, C.-C.; Wang, T.-I. Applying game mechanics and student-generated questions to an online puzzle-based game learning system to promote algorithmic thinking skills. *Comput. Educ.* **2018**, *121*, 73–88. [CrossRef]
40. Sanchez, D.R.; Langer, M.; Kaur, R. Gamification in the classroom: Examining the impact of gamified quizzes on student learning. *Comput. Educ.* **2020**, *144*, 103666. [CrossRef]
41. Goh, D.H.-L.; Razikin, K.; Lee, C.S.; Lim, E.P.; Chatterjea, K.; Chang, C.H. Evaluating the use of a mobile annotation system for geography education. *Electron. Libr.* **2012**, *30*, 589–607.
42. Cheung, S.Y.; Ng, K.Y. Application of the Educational Game to Enhance Student Learning. *Front. Educ.* **2021**, *6*, 79. [CrossRef]
43. Hair, J.F.; Black, W.C.; Babin, B.J. *Multivariate Data Analysis*; Prentice-Hall: Englewood Cliffs, NJ, USA, 2006.
44. Wu, W.-H.; Hsiao, H.-C.; Wu, P.-L.; Lin, C.-H.; Huang, S.-H. Investigating the learning-theory foundations of game-based learning: A meta-analysis. *J. Comput. Assist. Learn.* **2011**, *28*, 265–279. [CrossRef]
45. Maher, Y.; Moussa, S.M.; Khalifa, M.E. Learners on Focus: Visualizing Analytics Through an Integrated Model for Learning Analytics in Adaptive Gamified E-Learning. *IEEE Access* **2020**, *8*, 197597–197616. [CrossRef]