Journal of Business Research 179 (2024) 114685

Contents lists available at ScienceDirect

Journal of Business Research

journal homepage: www.elsevier.com/locate/jbusres

Gamification in workforce training: Improving employees' self-efficacy and information security and data protection behaviours

Paula Bitrián [a,*], Isabel Buil [b], Sara Catalán [a], Dominik Merli [c]

[a] Faculty of Business and Economics of the University of Zaragoza. Gran Vía 2, 50005, Zaragoza, Spain
[b] Faculty of Business and Economics of the University of Zaragoza. María de Luna, s/n - Edificio "Lorenzo Normante" – 50018, Zaragoza, Spain
[c] Faculty of Computer Science of the Augsburg University of Applied Sciences. An der Hochschule 1, 86161 Augsburg, Germany

ARTICLE INFO

Keywords:
Gamification
E-training
Information security
Data protection
Information system success
Phishing

ABSTRACT

This research aims to address two questions: (1) how can gamification strategies increase success of e-training systems and enhance employees' information security and data protection self-efficacy? and (2) do gamified e-training systems improve employees' information security and data protection behaviours? Drawing on the information systems success literature, this research offers new insights into gamified information security and data protection e-trainings through two studies. Study 1 analyses the perceptions of 1,178 employees of an international company using structural equation modelling. The results show that gamification significantly influences information quality, system quality and enjoyment which, in turn, increase perceived usefulness and satisfaction. Perceived usefulness also enhances satisfaction, and both variables improve security self-efficacy. Study 2 investigates the employees' behaviours by analysing their responses to phishing. The results confirm that gamified e-training improves employees' security behaviours, as it reduces the percentage of employees who click on a phishing attack and promotes positive reactions.

1. Introduction

Recent years have seen a significant increase in the number of cyberattacks and data breaches. The European Union Agency for Cybersecurity noted that "throughout the latter part of 2022 and the initial half of 2023, there was a notable escalation in cybersecurity attacks, setting new benchmarks in both the variety and number of incidents" (ENISA, 2023, p. 6). During the first quarter of 2023 alone, more than six million data records were exposed worldwide through data breaches (Statista, 2023a), costing, on average, $4.45 million per incident (IBM, 2023). In this context, it is not surprising that data protection – i.e. a set of measures adopted to protect personal data from improper use, loss and transfer – and information security – i.e. the processes and tools developed and implemented to ensure the confidentiality, integrity and availability of sensitive business information – have become high priorities for organisations (Andersson et al., 2022; Costa, 2020).

Information security and data protection incidents can have serious negative consequences, both internally, affecting organisations in terms of operations, workforce retention, legal issues and financial losses, and externally, impacting organisational image and reputation (Schlackl et al., 2022). Thus, organisations are increasingly investing in information security to protect their information assets (Andersson et al., 2022). Recent forecasts have predicted that the information security technology market will reach a value of $300 billion worldwide in 2030 (Statista, 2023b).

Despite these large investments in information security technologies and management systems, in many cases organisations fail to protect their information assets because they neglect the human factor (Khando et al., 2021). An effective defence against cyberattacks should combine processes and technology, but it also should include the human factor (Bellon, 2020). However, within organisations, people are often an overlooked, vulnerable link in the security system (Canham et al., 2022). The report *Voice of the CISO 2023* stated that 60 % of chief information security officers (CISOs) consider human errors to be their organisations' greatest vulnerability to cyberattacks. Similarly, the *2023 Data Breach Investigations Report* by Verizon (2023) posited that 74 % of data breaches involve a human element, while the World Economic Forum stated in *The 2022 Global Risks Report* that 95 % of all cyber security issues can be traced back to human error. Information security awareness is gaining greater importance as a means of mitigating information security risks (Rohan et al., 2021).

[*] Corresponding author.
E-mail addresses: pbitrian@unizar.es (P. Bitrián), ibuil@unizar.es (I. Buil), scatala@unizar.es (S. Catalán), dominik.merli@hs-augsburg.de (D. Merli).

https://doi.org/10.1016/j.jbusres.2024.114685
Received 21 November 2022; Received in revised form 24 March 2024; Accepted 24 April 2024
Available online 11 May 2024

Traditional methodologies used in information security and data protection training are, however, not always effective. Traditional training methods do not always provide engaging and appropriate materials (Khando et al., 2021; van Steen & Deeleman, 2021). In addition, employees often perceive email communications and instructor-led classroom sessions as distractions from the daily workload, thus rendering them ineffective in encouraging the adoption of appropriate information security behaviours (Silic & Lowry, 2020) and in increasing data protection awareness (Dincelli & Chengalur-Smith, 2020).

To overcome the limitations of traditional methods, many organisations have embraced gamification strategies. Gamification is proposed as a strategic tool to make learning an immersive experience that supports participants to practically apply their training (Aldalur & Perezt, 2023). Gamified learning environments have been shown to be more effective than traditional methodologies in supporting employee involvement in the training context and in making them aware of how to apply course content to real-world jobs (Kim, 2021). Certain gamification principles reshape descriptive teaching and include experiential activities where participants can learn in a risk-free environment (Wang et al., 2022). Therefore, gamification is increasingly being used in corporate employee training to redesign the training approaches (Wang et al., 2022). For instance, large organisations, such as Deloitte and PricewaterhouseCoopers (PwC), use gamification to train their employees on information security awareness.

Gamification has been defined as the application of game elements and mechanics (e.g. points, badges, feedback, challenges, leaderboards) to non-game contexts (Deterding et al., 2011) to promote in individuals a series of psychological outcomes, such as enjoyment and satisfaction, with the final goal of achieving desired behaviours (Koivisto & Hamari, 2019). For instance, employees can earn points by completing specific tasks, which can be used to encourage competition or as a feedback mechanism to show progression. Similarly, employee achievements, such as acquiring new skills, can be rewarded with badges. As an information systems (IS) phenomenon, gamification attempts to promote game-like experiences in utilitarian IS (Behl et al., 2022a; Koivisto & Hamari, 2019). In the online context, it has been shown to be an excellent strategy for enhancing education, brand engagement and IS engagement (Jayawardena et al., 2021). Gamification strategies can also help companies in digital transformation (Behl et al., 2022b), increase employee engagement (Pereira et al., 2022), enhance innovative performance in the workplace (Behl et al., 2022c) and even improve the company's environmental sustainability (Behl et al., 2023).

In the information security and data protection context, gamified training systems are very diverse and may have various designs. These methods can be grouped into three main categories: employee training platforms, serious games and computer security competitions (e.g. Capture the Flag challenges). While employee training platforms incorporate game elements, such as points, badges and leaderboards, to enhance the training experience (e.g. Baxter et al., 2016; Petrykina et al., 2021; Thornton & Francia III, 2014), serious games are fully developed games and are not for entertainment purposes (e.g. Hendrix et al., 2016). Finally, in computer security competitions, such as the Capture the Flag challenges (e.g. Boopathi et al., 2015; Karagiannis & Magkos, 2020), participants, either individually or in groups, are challenged to, for example, find and exploit vulnerabilities in a system. Prior studies have posited that the implementation of gamification in information security training systems in organisations leads to positive employee-related results, such as experiential and active learning, deeper understanding, higher intrinsic motivation and better security policy compliance (e.g. Banfield & Wilkerson, 2014; Baxter et al., 2016; Dincelli & Chengalur-Smith, 2020; Silic & Lowry, 2020).

However, despite these positive outcomes, major challenges and limitations remain in this area of research that need to be addressed. First, as Chen et al. (2023) recently noted, there is a lack of empirical studies analysing the influence of gamification in information security education. Previous literature has not provided clear empirical evidence about the effectiveness of gamification in enhancing employee perceptions of security self-efficacy, that is, their perceptions of having the abilities and knowledge to properly engage in appropriate information security behaviours and contend with security incidents (Silic & Lowry, 2020). Many studies have discussed the effectiveness of gamification in information security education from a theoretical viewpoint (e.g. Adams & Makramalla, 2015; Wolfenden, 2019), while others have focused mainly on designing, and experimenting with, gamified systems to provide information security information, offering only preliminary results on their effectiveness (e.g. Alqahtani & Kavakli-Thorne, 2020; Boopathi et al., 2015; Ghazvini & Shukur, 2018; Hart et al., 2020; Thornton & Francia III, 2014; Yamin et al., 2021; Yasin et al., 2018). Given that the effects of gamification are highly dependent on both the context in which the strategy is implemented and on the users employing it (Hamari et al., 2014), empirical studies exploring its use in this field are needed to verify its effectiveness. In addition to investigating whether gamification works, it is important to understand how it leads to the expected outcomes. However, as Silic and Lowry (2020) noted, most studies in this context have not used theoretical foundations to explain gamification effectiveness. There is thus a need for more empirical studies that, drawing on solid theoretical foundations, explore whether, and how, gamification can enhance information security education and behaviours. Second, the literature on organisational information security has revealed an important data-gathering limitation, that is, organisations are generally reluctant to provide information security-related data due to sensitivity concerns (Kweon et al., 2021). In this sense, most studies have used samples of students and, therefore, have neither analysed actual working gamified training nor actual organisations (e.g. Alqahtani & Kavakli-Thorne, 2020; Banfield & Wilkerson, 2014; Bioglio et al., 2019; Karagiannis & Magkos, 2020; Petrykina et al., 2021; Thornton & Francia III, 2014; Wu et al., 2021; Yasin et al., 2018, 2019). This makes it difficult to apply and generalise the results of the studies to the corporate context, as employees, in comparison to students, must deal with different tasks and may have different motivations to learn (Silic & Lowry, 2020). Finally, with some exceptions (e.g. Canham et al., 2022; Silic & Lowry, 2020), few studies have objectively measured the improvement in employees' actual information security behaviours after completing gamified e-training. As van Steen and Deeleman (2021) argued, future research should examine the effects of gamified cyber security training using objective behavioural measures, that is, not only self-reported behaviour and individuals' perceptions.

In two studies we aim to address the gaps identified above and offer new insights into the effectiveness of gamified e-training on information security awareness and data protection. In particular, this study aims to address two key research questions (RQs):

- ***RQ1****: How can gamification strategies increase the success of e-training systems and enhance employees' information security and data protection self-efficacy?*
- ***RQ2****: Do gamified e-training systems improve employees' information security and data protection behaviours?*

In Study 1, we answer the first question and explore how gamification embedded in e-training systems can increase their success and enhance employees' perceptions of security self-efficacy. To achieve this objective, a research model based on the IS success literature (DeLone & McLean, 1992, 2003; Seddon, 1997; Seddon & Kiew, 1996) and, more specifically, on Seddon's sub-model of IS success (Seddon, 1997), is proposed. The IS success literature provides a comprehensive framework for evaluating the success of IS and has been used to appraise gamified interventions and explain the effects of gamification (Aparicio et al., 2019). Therefore, drawing on Seddon's (1997) model, we analyse how gamification improves information quality and system quality, and how it fosters participants' enjoyment of e-training systems. In addition, we examine the influence of information quality, system quality and enjoyment on employees' perceptions of the usefulness of the system and employee satisfaction. Finally, we analyse how perceived usefulness enhances employee satisfaction and how these factors improve employees' perceptions of security self-efficacy. Study 1 explores the subjective perceptions of the employees of a large international company collected through a self-reported questionnaire. Structural equation modelling was used to test the hypotheses of the proposed model. The results suggested that gamification increases the success of e-training systems and enhances employees' security self-efficacy.

In Study 2, we address the second research question and examine the effectiveness of gamified e-training on information security awareness by analysing employees' responses to a phishing attack. Study 2, therefore, complements the results obtained in Study 1, by examining employees' actual behaviours in the same international company. The results showed that gamified information security e-training systems enhance employees' security behaviours.

This study contributes to the literature in several ways. First, gamification is underrepresented in the IS literature (Koivisto & Hamari, 2019). Therefore, this study contributes to the IS success literature by examining the role played by gamification as an antecedent of IS success under a mandatory use context within an organisation. Second, this research provides valuable insights into the gamification literature (Koivisto & Hamari, 2019; Rapp et al., 2019) in general, and the security gamification literature (Silic & Lowry, 2020) in particular. While gamification has been examined in different contexts, scholars have called for research to empirically analyse its use for employee information security training (Chen et al., 2023; Silic & Lowry, 2020). Therefore, this study provides new insights by empirically analysing the effects of game elements embedded in gamified information security and data protection e-training. Finally, the study not only looks at employees' perceptions but also answers the call in the literature to objectively analyse their security behaviours (van Steen & Deeleman, 2021) by conducting a phishing campaign to measure improvements in employee information security behaviours.

This research also offers practical implications to cyber professionals, developers and providers of this type of educational and training content. First, it highlights the importance of employee training in improving their information security-related behaviours. In addition, it shows the effectiveness of using gamification strategies to enhance the training experience. Specifically, game elements, such as challenges, clear goals, feedback and a narrative context, enhance the success of e-training systems and, in turn, increase employees' awareness and perceptions of having the ability to perform appropriate information security behaviours, that is, their security self-efficacy.

2. Previous gamification studies related to information security and data protection

More and more organisations are using gamification to train employees in information security and data protection (Hart et al., 2020; Silic & Lowry, 2020; van Steen & Deeleman, 2021). As previously noted, human error plays an important role in information security incidents. Therefore, investments in information security technologies are not effective if people lack information security awareness (Khando et al., 2021). For this reason, a key objective of information security research has been to explore ways to enhance users' decisions about information security practices and motivate them to effectively protect sensitive information (Vedadi et al., 2021). Some studies have highlighted that one way to improve compliance with a company's information security policies is by introducing financial incentives in the form of extrinsic rewards (Goel et al., 2021). For instance, employees can earn an extra bonus if they comply with the company's information security policies; alternatively, they could receive the monetary bonus but lose part of it if they make a mistake. In particular, Goel et al. (2021) confirmed that compliance with information security policies regarding phishing emails was higher when participants were told that noncompliance would reduce their rewards (i.e. negative or loss framing) than when compliance would increase their rewards (i.e. positive or gain framing). Other studies, however, have suggested that including game elements (i.e. points, avatars, game master, notifications, trophies) in information security training systems encourages positive outcomes. For instance, gamified interactive security systems, which reward users with points, display the user's status and present notifications about their behaviours, can help prevent the download of malware (Petrykina et al., 2021). In addition to points, social gamification features such as competitions can promote positive employee behaviours (e.g. the timely identification of phishing attacks) (Canham et al., 2022). Silic and Lowry (2020) found that the use of game elements such as avatars, points, badges, levels, game masters, immediate feedback and leaderboards can also lead to positive behavioural changes. Similarly, in a quasi-experimental study, Wu et al. (2021) found that gamified learning systems that incorporate game elements such as avatars, points, leaderboards, rewards or challenges are more effective in promoting information security knowledge than conventional lecture-based classrooms. Specifically, the results indicated that gamification enhanced learners' information security knowledge in the specific areas of password management, Internet use and information handling. Indeed, gamification used to develop information security skills does not attempt to convey theoretical concepts but rather is used to promote experiential learning, which makes it more difficult for learners to forget the knowledge acquired (Banfield & Wilkerson, 2014; Silic & Lowry, 2020).

Table 1 contains an up-to-date review of the relatively few studies that have investigated gamification in the information security and data protection context. The gamified systems that have been proposed/designed to provide training and education in information security and data protection are very diverse. Table 1 groups them into three main categories. First, many online training systems incorporate game elements, such as feedback, narrative context, levels, competition, scores, leaderboards and rewards (e.g. Baxter et al., 2016; Canham et al., 2022; Chen et al., 2023; Dincelli & Chengalur-Smith, 2020; Petrykina et al., 2021; Silic & Lowry, 2020; Thornton & Francia III, 2014), to enhance the learning experience. More specifically, game elements and mechanics are used in the training process to promote information security and data protection behaviours, such as defending against phishing attacks (Canham et al., 2022; Silic & Lowry, 2020), and to address data protection issues (Dincelli & Chengalur-Smith, 2020).

The second group involves serious games, which are considered by some authors as a subset of gamification (e.g. Kapp, 2012). Serious games are very popular in information security training (Hendrix et al., 2016). They can take the form of board games (e.g. Hart et al., 2020), augmented reality games (e.g. Alqahtani & Kavakli-Thorne, 2020), card games (e.g. Yasin et al., 2018, 2019), simulation and casual genre games (e.g. Ghazvini & Shukur, 2018) and computer games (e.g. van Steen & Deeleman, 2021). Briefly, board games provide realistic scenarios where participants can learn about cyber security topics from the perspective of attackers and defenders in a risk-free environment. Hart et al. (2020) noted that employee perceptions about using these games for information security training were positive. Second, augmented reality games enhance users' experience by combining the real world with computer-generated content and providing feedback to teach cyber security concepts and also show the consequences of cyber security attacks. These games are easy to use, increase individuals' cyber security awareness and enhance knowledge of cyber security threats and solutions (Alqahtani & Kavakli-Thorne, 2020). Third, in multiplayer card games cooperation within the team is essential, but at the same time, teams compete against each other. The training is framed within a story that develops attack scenarios where the teams face certain challenges. These games can be an effective learning methodology for teaching security concepts and can promote positive learning outcomes, engagement and participation (Yasin et al., 2019). Simulation and casual genre games simulate real work environments while combining them with flexibility

Table 1
Gamification Studies Related to Information Security and Data Protection.

Reference	Aim	Gamification system	Research design	Variables studied	Participants/ sample size	Key findings
Game elements embedded in a training platform						
Thornton & Francia III (2014)	To develop a gamification tool for information systems and information security training; to discuss the tool's viability based on preliminary results	Game elements embedded in a training platform	Survey	Motivation, attendance, awareness	150 students/ student control group	Gamified tools showed relatively promising benefits: the results showed positive attitudes towards the interventions and improved attendance and success rate
Baxter et al. (2016)	To examine if a gamified training environment promotes higher trainee satisfaction and knowledge acquisition	Game elements embedded in a training platform	Laboratory experiment Field study	Satisfaction and knowledge acquisition	Study 1: 33 students in True Office company, 38 in Thomson Reuters group, 45 in control group Study 2: 856 employees	Gamification enhanced satisfaction in the lab and field studies but showed only marginally significant improvements in knowledge acquisition
Dincelli & Chengalur-Smith (2020)	To create a gamified security education, training and awareness (SETA) artefact, to identify the security threats to which trainees are most susceptible and to facilitate behavioural change	Gamified security education, training and awareness artefact	Empirical/ quantitative (experiment and survey)	Instrumental outcomes (attitudes, intentions and online self-disclosure (OSD) behaviours), experiential outcomes (memorability and user experience)	1,718 employees	This gamified SETA intervention is an innovative solution which is more effective than current solutions to the problem of OSD behaviours, which can lead to security threats. The results also showed that of the gamified interventions the text-based artefact was better at improving instrumental outcomes, and the visual-based artefact was better at improving experiential outcomes.
Silic & Lowry (2020)	To create a gamified security training system to enhance intrinsic motivation and security learning and efficacy To propose a hedonic-motivation system adoption model which assesses security-related constructs, employees' intrinsic motivations and their ability to cope with security challenges, to positively change their behaviours	Game elements embedded in a training platform	Empirical/ quantitative (survey and experiment) Structural equation modelling	Perceived ease of use, perceived intrinsic usefulness, curiosity, joy, control, challenge, learning, security response efficacy, security self-efficacy, immersion, behavioural intention to follow security policies, actual phishing response following security policies	420 employees	Game elements can improve organisational security training systems, providing intrinsic motivation to learn and comply with security measures, and provide the efficacy necessary for employees to actually carry out appropriate anti-phishing behaviours. All the hypotheses were supported except the relationship between joy and behavioural intention.
Petrykina et al. (2021)	To develop and describe a gamified interactive security system that rewards users based on their online security behaviours To evaluate its effectiveness compared to traditional security messages	Game elements embedded in a training platform	Empirical/ quantitative (experiment)	Productivity and security	94 students	The gamified experience decreased the volume of downloaded malware without harming productivity; presenting pre-emptive notifications enhanced this effect
Wu et al. (2021)	To examine the effect of a gamification practice on students' information security awareness knowledge improvement, attitude and intention of security compliance and willingness for continuous information security education	Game elements embedded in a training platform	Empirical/ quantitative (quasi-experimental study)	Information security awareness knowledge enhancement, attitude, intention of security compliance and willingness for continuous information security education	110 students	Students within a gamified class performed better than students within a lecture-based class. Gamification significantly influences the three security areas of password management, Internet use and information handling. However, gamification does not influence the attitude and intention of security compliance and willingness for continuous information security learning.
Canham et al. (2022)	To evaluate the success of gamified phishing training, focusing on employees' positive behaviours and to analyse differences in	Gamified phishing attacks	Empirical/ quantitative (experiment)	The Big Five personality dimensions, learning, prove performance and avoid performance	101 employees from a university	Past performance on simulated phishing campaigns positively predicted Phish Derby performance; older

(continued on next page)

Table 1 (*continued*)

Reference	Aim	Gamification system	Research design	Variables studied	Participants/ sample size	Key findings
	performance depending on sociodemographic variables and the Big Five personality dimensions					participants performed better, but more educated participants performed worse; and individuals who used a mix of personal computers and Macs at work performed worse than those using a single platform. Extraversion and agreeableness were associated with poorer performance in phishing detection and reporting. Likewise, individuals who were driven to perform well in the Phish because they wished to learn from the experience performed at a lower level than those driven by other goals. Interestingly, self-reported levels of computer skill and the perceived ability to detect phishing messages failed to exhibit a significant relationship with Phish performance.
Chen et al. (2023)	To propose and test a research model to analyse the effect of a gamified information security education system (ISES) on information on increasing information security awareness and protection behavioural intention	Game elements embedded in a training platform	Empirical/ quantitative (survey)	Enjoyment affordance, knowledge affordance, physical presence, information security knowledge growth, information security awareness, information security protection intention	220 students and employees	(1) The affordance of the gamified ISES may increase users' information security awareness through both emotional and cognitive paths. (2) Information security awareness increases information security protection behavioural intention, but physical presence and information security knowledge do not increase it. (3) Interest-type curiosity positively moderates the relationship between enjoyment affordance and physical presence, and deprivation-type curiosity positively moderates the relationship between knowledge affordance and the increase in information security knowledge.
Serious games						
Adams & Makramalla (2015)	To describe a gamification method from an attacker's perspective to develop cyber security skills among an organisation's employees and leaders	Serious game: Attack and defence game play	Discussion paper	Cyber security skills	N/A	The combination of gamification, an entrepreneurial perspective and attacker-type streams allowed trainees to experience an attack through the eyes of a cyber-attacker and develop cyber security skills
Ghazvini & Shukur (2018)	To design a serious game (InfoSecure) to improve information security awareness in the healthcare sector	Serious game: Simulation and casual genre game	Empirical/ qualitative (record of playing; pilot test)	Employee performance	5 students 5 employees	Employees found the serious game interactive and enjoyable. The level of employee information security awareness increased after playing the serious game. In addition, employees showed a greater willingness to participate in information security awareness training as they had a pleasant time playing the game.

(continued on next page)

Table 1 (*continued*)

Reference	Aim	Gamification system	Research design	Variables studied	Participants/ sample size	Key findings
Yasin et al. (2018)	To design a serious game to improve security awareness and evaluate the game's effectiveness	Serious game: Card game	Empirical/ quantitative and qualitative (survey and observation)	Perceived fun to play, perceived ease of playing, perceived intention to play, collaborative learning, learning performance, helps in security requirements elicitation	16 Students Lab study	Serious games can be an effective and fun way of learning security concepts, replicating real-life problems and making them more understandable, and motivating individuals to learn
Wolfenden (2019)	To discuss how gamification in the form of Cyber Ranges is gaining importance as a learning strategy in cyber security	Serious game: Cyber Range	Discussion paper	N/A	N/A	Gamified learning is evolving the cyber security industry and, along with innovations and advances in artificial intelligence and machine learning, security professionals are paving new pathways to address cyber security issues
Yasin et al. (2019)	To design and evaluate a serious game to teach software security concepts and make the learning experience more engaging	Serious game: Card game	Empirical/ qualitative (survey, brainstorming and observation)	Fun to play, ease of playing, intention to play, game-based learning, cyber security knowledge and avoidance behaviour	96 students	The serious game had a positive impact on players' security learning outcomes, engagement and participation. Game-based learning may be an effective methodology for teaching security-related concepts.
Alqahtani & Kavakli-Thorne (2020)	To develop an augmented reality (AR)-based serious game to increase cyber security awareness and knowledge and to evaluate and test its effectiveness for cyber security education	Serious game: An augmented reality game	Experimental study (survey) Descriptive analysis	Learning, fun, motivation. Perceived ease of playing, continuous use	91 undergraduate students	The augmented reality game for cyber security awareness was engaging and increased understanding of cyber security attacks and vulnerabilities. The results highlighted three main benefits: it is very easy to play, it supports individuals' cyber security awareness and it facilitates understanding of cyber security issues and solutions.
Hart et al. (2020)	To propose a serious game to increase cyber security awareness for people with non-technical backgrounds working in organisations, and to assess the perceived efficacy of the game for increasing cyber security awareness	Serious game: Board game	Empirical/ quantitative (4 experiments and survey)	Perceived ease of use, perceived usefulness, intention to use	1st experiment: 14 undergraduate students 2nd experiment: 15 students 3rd experiment: 12 employees 4th experiment: 13 legal practitioners and lawyers	Employees are more confident than students that serious games can improve their awareness of cyber security issues. Employees enjoyed the game rules and mechanics; however, the students did not enjoy playing the game.
Luh et al. (2020)	To propose and test a *meta*-model designed to provide a complete view of information system attacks and their reduction and a tool for security education	Serious game: Attack and defence game play	Quantitative (experiment, survey)/ Qualitative (interviews)	Knowledge gain, attack categories, game evaluation (accessibility, balance and design) and model evaluation	Higher education environment	The gamified model defines a wide range of actors, assets and actions. It allows the evaluation of cyber risks while allowing technical experts to explore specific attack scenarios in the context of an abstract IT infrastructure. The serious game prototype was successfully tested in a higher education environment.
van Steen & Deeleman (2021)	To design a serious game for cyber security training and test its efficacy compared to a non-cyber security-based game, incorporating factors of the theory of planned behaviour (TPB)	Serious game: Computer game	Empirical/ quantitative (experiment; survey)	Attitude, subjective norms, perceived behavioural control, intention, self-reported behaviours	258 participants (Employees and students)	The cyber security game showed higher self-reported scores on attitudes, perceived behavioural control, intentions and behaviour than did non-cyber security games
Yamin et al. (2021)	To develop and evaluate a serious game which simulates cyber security exercise scenarios where players can act as cyber attackers or	Serious game: Attack and defence game play	Empirical/ survey	Realism and efficiency	25 participants	The game realistically represented the cyber security exercise scenario

(continued on next page)

Table 1 (*continued*)

Reference	Aim	Gamification system	Research design	Variables studied	Participants/ sample size	Key findings
	defenders in a multiplayer environment					
Capture the Flag challenge						
Boopathi et al. (2015)	To introduce a gaming approach to learning cyber security skills by developing a game, and to test students' knowledge at each level of the game	Capture the Flag challenge	No empirical study conducted	Security knowledge level	N/A	Introducing a gaming approach to cyber security education (such as a Capture the Flag security competition) creates an effective tool to train in computer security and for developing a secure online world
Karagiannis & Magkos (2020)	To show the potential of Capture the Flag challenges for enhancing the learning experience and improving students' skills and knowledge	Capture the Flag challenge	Empirical/ quantitative (experiment, survey)/ Qualitative (experiment, observation)	Perceived learning, self-directed learning, assessment capabilities, attention, relevance, confidence and satisfaction	32 undergraduate students for the pre-engagement survey (to select the appropriate Capture the Flag challenge) 25 to 30 students for the observation research during the lab experiment	Students showed higher confidence in their skills and were more engaged during the learning experience. The outcomes related to technical skills and knowledge acquisition were positive.

Note: N/A: Not applicable.

and fun, and have been found to increase employee information security awareness (Ghazvini & Shukur, 2018). Computer games can entail solving different tasks related to cyber security incidents and incorporate increasing difficulty levels and scoring systems (van Steen & Deeleman, 2021). Another popular serious game design is information security attack and defence games (e.g. Adams & Makramalla, 2015; Luh et al., 2020; Yamin et al., 2021). In these competitive games, one team creates threats and attacks another team to steal its business information, while the second team builds defences and responds to the cyber security attacks. Finally, Cyber Ranges are an example of serious games that, through virtual platforms, simulate real-world scenarios, so that employees can interact with real threats in a risk-free environment (e.g. Wolfenden, 2019).

Finally, the third category comprises "Capture the Flag" challenges, which are popular tools for providing information security training and education (e.g. Boopathi et al., 2015; Karagiannis & Magkos, 2020). This training methodology can have different formats. In the "jeopardy" style, participants must complete various challenges and solve a set of questions. The game is divided into unlockable levels corresponding to different information security topics (e.g. basic programming skills, web application security concepts, reverse engineering) (Boopathi et al., 2015). Meanwhile, the "attack-defence" style involves teams attacking other teams and protecting their own systems. Each team has flags in the system that they must protect. If a team successfully attacks another team, they capture these flags and win points.

The focus of the present study is on the use of specific game elements: challenges, clear goals, narrative context and feedback, in an online training system. The choice of these game elements, as explained later, was based on the gamified system analysed in this study, which was developed by a company that specialises in gamified awareness training.

3. Hypotheses development and theoretical framework

3.1. Employees' perceptions of gamified information security and data protection e-training systems

Researchers have used a variety of theories to explain how gamification works. Self-determination and flow theory are two of the most commonly used (see Krath et al., 2021, for a detailed systematic review and analysis of the theoretical basis of gamification). The present study, however, draws on the IS success literature as it provides a comprehensive framework for evaluating the success of IS and has been used to evaluate gamified interventions (Aparicio et al., 2019).

Over previous decades, special attention has been paid to identifying the factors that contribute to IS success. The study by DeLone and McLean (1992) is considered one of the most influential in this field. The authors reviewed different measures of IS success and developed a six-dimensional taxonomy: system quality, information quality, use, user satisfaction, individual impact and organisational impact. These categories form the well-known Delone and McLean IS success model. Since its publication, the model has been tested, modified and updated (see DeLone & McLean, 2003).

Seddon and Kiew (1996) made one of the first attempts to empirically test the DeLone and McLean (1992) model. They proposed an alternative version in which usefulness replaced system use, arguing that usefulness is a better measure of IS success in mandatory contexts and in situations where a system is not in continuous use. When the use of a system is mandatory, however, the number of hours it is used provides little information about its usefulness and, therefore, the success of the system. Nevertheless, usefulness remains an important measure of success, as it indicates the extent to which a person perceives that the use of a specific system will improve his or her performance (Davis, 1989). In addition, the variable "system importance" was added to the model to explain variations in users' perceptions of usefulness and user satisfaction. According to Seddon and Kiew (1996), if the system supports a task that is perceived to be very important, the system will be perceived as useful. Finally, the simultaneous causality between use and user satisfaction included in the original DeLone and McLean (1992) model was replaced by one-way causality (i.e. usefulness causes user satisfaction). Seddon and Kiew (1996) argued that when the user perceives an IS to be more useful (s)he will feel more satisfied with it, but not the other way around, because "satisfaction reflects a wider set of expected benefits or aspirations than mere usefulness" (p. 95).

Subsequently, Seddon (1997) proposed a re-specified IS success model that included two different variance sub-models, a partial behavioural model of IS use and the IS success model. The partial behavioural model of IS use suggests that IS use is predicted by the user's expectations concerning the net benefits of future IS use. Furthermore, Seddon (1997) referred to IS use as a behaviour (i.e. not a success measure) which may have individual, organisational and/or societal consequences. Meanwhile, the IS success model includes three types of variables: (1) measures of information and system quality; (2) general perceptual measures of the net benefits of IS use (i.e. perceived usefulness and user satisfaction); and (3) other measures of the net benefits of

IS use. In this sub-model, information quality and system quality influence perceived usefulness and user satisfaction, perceived usefulness influences user satisfaction and, finally, the net benefits for individuals, organisations and society are expected to influence perceived usefulness and user satisfaction. Therefore, Seddon (1997) included perceived usefulness as a success measure but regarded IS use as a behaviour.

In the present study Seddon's sub-model of IS success, more specifically its measures of information and system quality, and the general perceptual measures of the net benefits of IS use (i.e. perceived usefulness and user satisfaction), serve as the basis for the proposed model. As depicted in Fig. 1, the research model explores the role of gamification as a success determinant in the context of e-training systems to promote information security and data protection. As such, it proposes that gamification influences information quality, system quality and enjoyment. In addition, it examines the influence of information quality, system quality and enjoyment on perceived usefulness and employee satisfaction. Finally, it analyses the relationship between perceived usefulness and employee satisfaction and whether these two IS success measures improve employees' security self-efficacy.

The effect of gamification on two of the IS success measures, information quality and system quality, and on enjoyment, is first explored. In the IS field, information and system quality are considered key dimensions of success and effectiveness (DeLone & McLean, 1992, 2003; Seddon, 1997; Seddon & Kiew, 1996). In e-learning environments, information quality refers to useful, understandable and reliable content delivered through learning management systems (Al-Fraihat et al., 2020; DeLone & McLean, 1992). Displaying information and content in a logical and comprehensible manner in learning courses helps participants achieve learning goals faster (Al-Fraihat et al., 2020). In this sense, game elements, such as challenges, clear goals, feedback and narrative, may simplify learning content and adapt it to the learners' abilities and knowledge (Krath et al., 2021). For example, gamification makes it possible to convey learning content through a narrative (Küpper et al., 2021). Transmitting learning content through stories with specific plots may also help disaggregate it into smaller topics (Wee & Choong, 2019). Similarly, reframing content in a meaningful narrative may help individuals to immerse themselves in the activity (Koivisto & Hamari, 2019). The feedback offered by gamified systems in the form of awarding points, reporting progress and through comments (Fu et al., 2009) supports instructional content (Krath et al., 2021; Laine & Lindberg, 2020). As such, instructional content can be complemented by information provided based on players' inputs, so that they receive feedback on their actions (Laine & Lindberg, 2020). In the information security educational context, gamification can reshape how training content is presented and help keep it updated. For instance, by representing real-life problems clearly and understandably (Yasin et al., 2018) and by modelling attack and defence scenarios (Yamin et al., 2021). In sum, game design elements and mechanics are powerful tools for communicating information (Rodrigues et al., 2017) and supporting pre-existing instructional content (Landers, 2014).

System quality refers to technological characteristics, ease of use, functionality and flexibility (Al-Fraihat et al., 2020; DeLone & McLean, 2003). Including too many features in e-learning systems can induce users to become frustrated with the relevant technologies, potentially leading to system abandonment (Sun et al., 2009). Therefore, together with information quality, system quality is considered one of the drivers of e-learning quality (Al-Fraihat et al., 2020) and is crucial for participants to enjoy a good learning experience (Cidral et al., 2018). The inclusion of gamification helps users navigate systems and supports their decision-making by quantifying their activities within the IS itself (Koivisto & Hamari, 2019; Rodrigues et al., 2017). Game elements, such as points, badges and leaderboards, facilitate the user experience by making it more comfortable, less frustrating and less effortful (García-Jurado et al., 2021). Gamification also reframes tasks and activities with game elements, such as by communicating clear goals which divide the main activity into smaller activities, by giving immediate feedback to report achievements and by creating a mutually supportive social community (Koivisto & Hamari, 2019). Providing continuous challenges and immediate feedback clarifies individuals' development and, therefore, helps to ensure that users do not become bored or overwhelmed by the activity (Csikszentmihalyi, 1975).

Finally, perceived enjoyment refers to the extent to which interacting with a system is perceived as enjoyable in itself (Davis, 1989). Incorporating game elements into IS provides hedonic benefits, such as enjoyment (Högberg et al., 2019). Prior research has posited that game elements, such as challenges (Mulcahy et al., 2020), rewards/badges (Zhang et al., 2021) and clear objectives and feedback (de Almeida & dos Santos Machado, 2021), can enhance users' feelings of enjoyment. Similarly, employing serious games to address information security may help users achieve their learning objectives in an interactive and fun way (Ghazvini & Shukur, 2018; Yasin et al., 2018). Gamification is useful in learning and training contexts because it can build enthusiasm, provide feedback on performance, give recognition to learners and encourage goal setting (Bai et al., 2020). In addition, incorporating gamification into the work environment not only leads to the enjoyment of a specific working task but also increases work enjoyment in general (Gerdenitsch et al., 2020).

Therefore, based on the arguments set out above, we expect that using a gamified e-training system in information security and data protection training will improve employees' perceptions of the system's

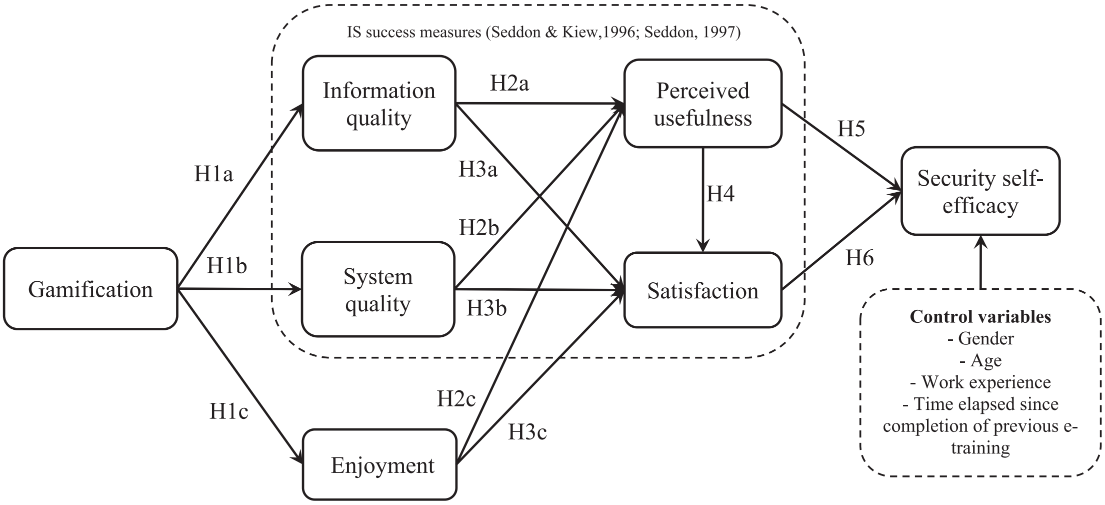

Fig. 1. Proposed model.

information quality, system quality and enjoyment. Accordingly, the following hypotheses are proposed:

H1a: Gamified e-training enhances employees' perceptions of information quality.

H1b: Gamified e-training enhances employees' perceptions of system quality.

H1c: Gamified e-training enhances employees' enjoyment.

The relationship between information quality, system quality, enjoyment and perceived usefulness is explored next. Perceived usefulness captures the degree to which an individual believes that the use of a particular system will improve his/her performance (Davis, 1989). In the literature on IS success, information quality and system quality have been related to usefulness (Seddon & Kiew, 1996). In particular, perceived usefulness has been considered a better measure of IS success than system use, especially when system use is mandatory (Seddon & Kiew, 1996; Seddon, 1997).

Previous studies in the online learning context have also examined the positive impact of information quality and system quality on perceived usefulness. Online courses with logical, understandable, up-to-date and accurate information, in a readable and attractive format, are perceived as more useful for achieving learning goals (Al-Fraihat et al., 2020; Lwoga, 2014). In addition, users regard technological systems as more useful when they perceive them as easy to use and operate (Lee et al., 2019; Manis & Choi, 2019). This positive relationship between perceived ease of use and usefulness has been found in several contexts, such as e-learning (Szymkowiak & Jeganathan, 2022), massive open online courses (Joo et al., 2018), learning management systems (Eraslan Yalcin & Kutlu, 2019) and computer-supported collaborative learning (Muñoz-Carril et al., 2021). Prior research has also shown that system quality is an important factor in users' perceptions of the usefulness of e-learning systems (Lwoga, 2014) and of their technical quality, which involves aspects such as system reliability, flexibility, availability and ease of use (Al-Fraihat et al., 2020). Thus, both information quality and system quality lead to systems being perceived as more useful.

Prior research has also highlighted the important role of fun and pleasure in enhancing perceived usefulness in contexts such as education (Abdullah et al., 2016), mobile games (Ha et al., 2007), mobile technologies (Alalwan et al., 2018), banking technologies (De Oliveira et al., 2019), augmented/virtual reality technologies (Holdack et al., 2022; Lee et al., 2019; Manis & Choi, 2019) and travel review sites (Wang & Li, 2019). Having an enjoyable experience when using distance e-learning systems boosts users' perceptions of the usefulness of the systems (Rizun & Strzelecki, 2020). Similarly, Syahruddin et al. (2021) found that enjoyment and pleasure experienced while interacting with e-training systems promote users' perceptions of their usefulness. Therefore, it is proposed that if individuals perceive that interacting with technology is enjoyable, they will regard the technology as more productive and beneficial.

Thus, the following hypotheses are proposed:

H2a: Information quality enhances employees' perceived usefulness of gamified e-training.

H2b: System quality enhances employees' perceived usefulness of gamified e-training.

H2c: Employees' enjoyment when using gamified e-training systems enhances the perceived usefulness of gamified e-training.

Satisfaction, which is associated with all the benefits that an individual expects to receive when using a particular IS (Seddon & Kiew, 1996), has also been considered to be an IS success measure (DeLone & McLean, 1992, 2003; Seddon, 1997; Seddon & Kiew, 1996). In IS success-related studies, information quality and system quality have been broadly related to user satisfaction (DeLone & McLean, 1992, 2003; Seddon, 1997; Seddon & Kiew, 1996). Previous literature in the context of e-learning has also found that information quality and system quality are determinant factors of learner satisfaction. Satisfaction is based on the positive experience that learners enjoy during their direct interaction with an e-learning system (Aparicio et al., 2016). Learner satisfaction is greater when e-learning systems provide interesting and understandable content and accurate, reliable and updated information (Al-Fraihat et al., 2020; Aparicio et al., 2019; Cidral et al., 2018). That is, educational management IS that can produce accurate and high-quality information increase user satisfaction (Martins et al., 2019). Similarly, when users find a system easy to use, and not technologically challenging, they pay more attention to the learning materials, given that less effort is required to master the technology; consequently, they derive greater satisfaction (Sun et al., 2008). Thus, system quality, as evidenced by a user-friendly and well-structured system, enhances user satisfaction with e-learning systems (Cidral et al., 2018; Lwoga, 2014). Distance learning students who perceive that the e-learning system they are using is highly technological will have higher perceived satisfaction (Bossman & Agyei, 2022). In addition, previous studies in the organisational context have shown that system quality affects employee satisfaction with e-learning and cloud systems (Chen, 2010; Donovan et al., 2018; Marjanovic et al., 2016).

IS designed to enhance user productivity are increasingly incorporating entertainment-oriented components to maximise user enjoyment (Koivisto & Hamari, 2019). As noted earlier, enjoyment is an intrinsic experience related to the extent to which using a system is perceived as enjoyable and pleasurable in itself, regardless of external outcomes. Hedonic values in mobile technologies, such as enjoyment, fun, pleasure and excitement, have a higher impact on user satisfaction compared to utilitarian values (Hsu & Lin, 2016; Lee & Kim, 2018). Yousaf et al. (2021) also found that experiencing enjoyment while interacting with technology enhances user satisfaction, while in the educational context, Muñoz-Carril et al. (2021) found that when students enjoyed using technology-based learning methodologies they experienced higher levels of satisfaction. Similarly, integrating components that promote enjoyment into workplace systems enhances job satisfaction (Silic et al., 2020).

Taking these arguments into account, the following hypotheses are proposed:

H3a: Information quality enhances employees' satisfaction with gamified e-training.

H3b: System quality enhances employees' satisfaction with gamified e-training.

H3c: Employees' enjoyment when using gamified e-training systems enhances their satisfaction

Seddon and Kiew (1996) argued that for users to be satisfied with an IS it must, at least, be useful. In distance learning, the perceived usefulness of e-learning systems has been identified as an important source of extrinsic learner satisfaction (Lwoga, 2014). Learners will be satisfied if they perceive that systems enable them to improve their learning performance and complete learning tasks faster (Al-Fraihat et al., 2020). Similarly, in the context of collaborative learning, when users perceive that computer-supported collaborative learning is useful for improving their individual learning, their satisfaction increases (Muñoz-Carril et al., 2021). Previous research has also demonstrated a positive relationship between the perceived usefulness of online learning systems and learner satisfaction (Al-Fraihat et al., 2020; Chen, 2010; Joo et al., 2018; Lwoga, 2014; Sun et al., 2008). Therefore, we expect that employees will feel more satisfied when they perceive that gamified e-training systems are useful. Accordingly, the following hypothesis is proposed:

H4: Perceived usefulness enhances employees' satisfaction with gamified e-training.

The effect of perceived usefulness and satisfaction on employee security self-efficacy is now examined. Self-efficacy refers to individuals' beliefs in their capacity to perform tasks and achieve given goals (Bandura, 1977). In the information security field, security self-efficacy has been defined as an employee's perception of having the necessary abilities and knowledge to carry out security behaviours, perform according to established policies and, therefore, face up to threats (Herath

& Rao, 2009; Silic & Lowry, 2020). Self-efficacy is an important measure of the effectiveness of training activities (Abraham & Chengalur-Smith, 2019). Thus, given the importance of security self-efficacy in reducing the risk of security threats, employees should be trained through security awareness programmes designed to promote a belief in their ability to perform the recommended security behaviours (Ng et al., 2009).

Previous literature on online learning system success has argued that increasing user perceptions of the usefulness of, and satisfaction with, systems will result in learners perceiving that they have increased their knowledge, achieved their learning goals and are more efficient in their learning tasks (Al-Fraihat et al., 2020). Similarly, satisfaction with e-learning is related to learner performance, that is, satisfied learners achieve better learning outcomes (Bossman & Agyei, 2022). In addition, in online collaborative learning contexts, the perceived usefulness of, and satisfaction with, learning methods have been found to positively impact students' perceptions of their learning (Muñoz-Carril et al., 2021). At the organisational level, prior studies have also shown that perceived usefulness and user satisfaction encourage learners to use the systems, which in turn improves overall job outcomes, such as task fulfilment, job satisfaction and job performance (Chen, 2010). Thus, it is expected that both the perceived usefulness of gamified e-training systems and employee satisfaction with the systems will increase their perceptions of having the ability to adopt effective information security behaviours. Therefore, the following hypotheses are proposed:

H5: Perceived usefulness of gamified e-training enhances employees' security self-efficacy.

H6: Employees' satisfaction with gamified e-training enhances their security self-efficacy.

The proposed research model analyses employees' perceptions of the training system and their beliefs in their capacity to adopt appropriate information security behaviours and cope with security incidents and threats. This step is key to understanding the effectiveness of information security training (Abraham & Chengalur-Smith, 2019), as a high level of security self-efficacy makes individuals more self-confident about their capabilities and skills (Tamjidyamcholo et al., 2013). However, while to achieve information security employees must perceive they have the necessary abilities and knowledge to engage in appropriate security behaviours, ultimate success depends on their actual behaviours (Rhee et al., 2009). Thus, the next section goes a step further by evaluating the effectiveness of the training course in behavioural terms by focusing on employees' information security behaviours after completing their e-training.

3.2. *Employees' actual behaviours*

When organisations have invested resources in, and implemented, information security training systems, they need to monitor whether or not they have had a real impact (Kweon et al., 2021) by assessing whether the security behaviours of their employees have significantly changed (Silic & Lowry, 2020). Therefore, in response to the second research question (RQ2: Do gamified e-training systems improve employees' information security and data protection behaviours?), this study also explores whether gamification engenders positive behavioural changes.

Gamification has the potential to impact the intra-organisational level by influencing employees' attitudes and behaviours (Wünderlich et al., 2020). The few studies that have analysed the impact of gamified learning on employees' information security-related behaviours have shown beneficial consequences, such as avoiding downloading malware (Petrykina et al., 2021) and identifying phishing attacks (Silic & Lowry, 2020).

Based on these previous findings, the present study investigates whether gamified e-training systems improve employees' actual behaviours. Employees' responses to a phishing attack were chosen as the objective and auditable security behaviour, for the following reasons. First, phishing attacks, which involve the sending of fraudulent communications, usually via email, appearing to come from a trusted and reputable source, are one of the most frequent information security threats in the business environment. For instance, in 2022, phishing was the most prevalent type of cybercrime reported to the United States Internet Crime Complaint Center (Statista, 2023c). They are also often used as the first move in cyberattacks and are one of the main causes of data breaches and security incidents (ENISA, 2017). Second, numerous organisations have adopted phishing simulations as part of their cyber security awareness training. One of the most effective preventive measures against phishing attacks is employee training (Iseni, 2021), which should not be aimed simply at preventing them from falling for phishing attacks but should also promote positive reactions from them that alert supervisors to potential threats (Canham et al., 2022). Finally, phishing simulations make it possible to measure employee behaviours, so that the employees' self-perceptions can be complemented with assessments of objective and auditable security behaviours. Therefore, we assess whether gamified e-training systems improve employees' responses to a phishing campaign.

4. Study 1

In Study 1 we tested the hypotheses of the proposed model to analyse whether gamification increases the success of e-training systems and employee security self-efficacy. To achieve this objective employees' subjective perceptions were explored by collecting data through a self-reported questionnaire.

4.1. *Method*

4.1.1. *Participants and procedure*

A cross-sectional non-experimental study was conducted to test the proposed model. Data were collected through an online survey using Microsoft Forms. The questionnaires were distributed among employees of a German multinational company. With a workforce of about 14,000, the company is a leading global provider in the engineering and high-tech sector in the Industry 4.0 environment, and is present in more than 50 countries. Prior to the data collection, the organisation's employees had completed gamified e-training courses in information security and data protection. Both topics are often affected by similar threats, vulnerabilities and risks. Given the similarities and overlaps in the employees' awareness of these two topics, organisations usually offer information security and data protection training courses, either separately or combined (Wlosinski, 2019). In the present study, training in information security and data protection was provided through two training courses, but both had identical structures and were undertaken by employees over the same period. The gamified e-training courses in information security and data protection were designed and developed by a well-known international company that specialises in the development and provision of customised employee awareness training for information security and data protection.

The course content was divided into chapters covering specific topics. Throughout the chapters, the training material explained the specific objectives of the course to inform the employees of what they needed to do to successfully complete the training. They were also given information about the objectives at the beginning of the learning experience. The chapters presented the training material using real and animated videos, providing real-world examples of potential breaches and threats. This type of narrative context encourages employees to become immersed in the activity. In addition, the training material was displayed through challenges, which consisted of practical exercises such as puzzles and drag-and-drop activities. While the employees navigated through the training materials, they received feedback and ratings on their achievements and progress, as well as notifications of their successes and failures. The four game elements of the gamified training identified – clear goals, narrative context, challenges and feedback – were analysed in the study.

After the company's works council had approved the study, the survey was conducted during February and March 2021. An invitation to complete the survey was sent to 8,930 employees from 11 different countries. The original questionnaire was in English, and it was translated into four languages (i.e. German, Spanish, Portuguese and Chinese). The different versions of the questionnaires were produced with the assistance of a professional translation agency. Of the 1,237 employees who responded to the survey, 1,178 returned valid responses. The characteristics of the sample are presented in Table 2.

4.1.2. Measures

The variables used in the study were measured using 7-point Likert scales based on previous literature (see Appendix A). Gamification was conceptualised as a second-order formative construct composed of four game elements measured as first-order reflective factors: challenges, feedback, clear goals and narrative context. Challenges were assessed following Silic and Lowry (2020); feedback and clear goals were measured following Fu et al. (2009); and narrative context used items adopted from Green and Brock (2000). To assess information quality, we adapted the scale of Aparicio et al. (2019). To assess system quality, we adopted items from Davis (1989) and Aparicio et al. (2019). Enjoyment was measured following Venkatesh (2000). Perceived usefulness was measured using items from Davis (1989). Satisfaction was assessed following Kettanurak et al. (2001), and security self-efficacy was assessed by adapting the scale of Silic and Lowry (2020). Finally, gender, age, time elapsed since completion of previous e-training and work experience in the company were included as control variables.

Table 2
Sample characteristics.

Category		Percentage (%)
Gender	Male	76.3 %
	Female	16.8 %
	Prefer not to say	6.9 %
Age	< 18 years old	0.3 %
	18–25 years old	4.8 %
	26–35 years old	23.1 %
	36–45 years old	24.4 %
	46–55 years old	24.7 %
	> 55 years old	16.4 %
	Prefer not to say	6.3 %
Type of e-training	Data Protection	5.8 %
	Information Security	2.9 %
	Both	91.3 %
Time elapsed since completion of previous e-training	< 1 month	19.3 %
	1–3 months	34.5 %
	3–6 months	21.7 %
	6 months to 1 year	17.7 %
	> 1 year	6.8 %
Location	Asia-Pacific (APAC)	14.4 %
	Europe, Middle East, Africa (EMEA)	66.3 %
	North, Central and South America (AMER)	19.3 %
Work experience	< 1 year	7.7 %
	1–5 years	29.9 %
	5–10 years	26.1 %
	> 10 years	36.3 %
Work area	Information Technology (IT)	7 %
	Human Resources (HR)	2.6 %
	Engineering	29.7 %
	Research	2.3 %
	Marketing	1.2 %
	Administration	5.2 %
	Development	12.1 %
	Manufacturing	16.2 %
	Finance	3 %
	Legal	0.3 %
	Sales	9.8 %
	Management	8.6 %
	Training	2 %

4.1.3. Common method bias assessment

The presence of common method bias was assessed using both procedural and statistical methods (Podsakoff et al., 2003). First, participation in the study was voluntary and anonymous. In addition, to prevent the respondents from identifying cause–effect relationships among the constructs the dependent and independent variables were included on different pages of the survey. Finally, a variance inflation factor (VIF) assessment suggested there was no common method bias: values ranged from 1 to 3.253, lower than the 3.3 threshold (Kock, 2015).

4.2. Results

Partial least squares structural equation modelling, with SmartPLS 3.0 software, was used to test the hypotheses (Ringle et al., 2015), for the following reasons: first, the measurement and structural models are complex; second, formatively and reflectively measured constructs are used in the research; and third, the data are not normally distributed (Hair et al., 2017a). The measurement model was first assessed, followed by the structural model. These two steps are described below.

4.2.1. Assessment of the measurement model

First, the reflective measurement model for the first-order dimensions was assessed (Hair et al., 2017b). Individual item reliability for all factor loadings was confirmed; they were all above 0.70 and statistically significant at 1 % (Carmines & Zeller, 1979) (Table 3). Construct reliability was confirmed as the Cronbach's alpha and composite reliability (CR) for all constructs were above the threshold of 0.7. The constructs also met the convergent validity criteria, as the average variance extracted (AVE) values were above 0.5 (Fornell & Larcker, 1981) (Table 3). Finally, to evaluate discriminant validity we verified that the outer loadings of all the indicators were higher than the respective cross-loadings (Hair et al., 2017b). We also proved that the square roots of the AVEs of each construct were greater than the inter-construct correlations (Fornell & Larcker, 1981) (Table 4). Finally, we confirmed that the normal bootstrap confidence interval of the heterotrait–monotrait (HTMT) criterion, with Bonferroni adjustment, did not contain the value 1 (Henseler et al., 2015).

Gamification was conceptualised as a second-order formative construct composed of four first-order factors: challenge, feedback, clear goals and narrative. Thus, the assessment of the first-order constructs was followed by the creation of a second-order construct using the two-stage approach proposed by Hair et al. (2018). The resulting model was re-estimated and re-evaluated. As can be seen in Table 5, the model has no multicollinearity problems as the VIF values range from 1.182 to 2.438 (Hair et al., 2011). Finally, the external validity of the model was also acceptable as the weights and loadings of the indicators were statistically significant and, therefore, they contributed to the construct (Hair et al., 2017b).

4.2.2. Assessment of the structural model

The statistical significance of the standardised paths was assessed through a bootstrapping process with 5,000 subsamples. The model explains 66 % of information quality variance, 52 % of system quality, 38.4 % of enjoyment, 58.6 % of perceived usefulness, 78.2 % of employee satisfaction and 46.1 % of security self-efficacy. To analyse predictive relevance, the Stone–Geisser test was carried out. The Q^2 values for the dependent variables were all positive, indicating the model has predictive relevance (see Table 3). Finally, the model has a good fit, since the standardised root mean square residual value was less than the threshold of 0.08 (Hu & Bentler, 1998).

Table 6 presents the results. Gamification was positively related to information quality ($\beta = 0.813$; $t = 60.098$), system quality ($\beta = 0.721$; $t = 33.276$) and enjoyment ($\beta = 0.620$; $t = 31.265$), supporting H1a, H1b

Table 3
Reflective measurement model results.

Construct	Indicator	Mean	Standard deviation	Factor loading	AVE	Cronbach's alpha	CR	Q^2
Challenges	CH1	4.29	1.66	0.941	0.893	0.881	0.944	N/A
	CH2	4.36	1.55	0.950				
Feedback	FE1	5.75	1.33	0.926	0.892	0.939	0.961	N/A
	FE2	5.90	1.28	0.959				
	FE3	5.91	1.29	0.948				
Clear goals	GO1	5.79	1.25	0.964	0.926	0.920	0.962	N/A
	GO2	5.78	1.28	0.961				
Narrative	NAR1	5.43	1.30	0.937	0.876	0.929	0.955	N/A
	NAR2	5.26	1.42	0.955				
	NAR3	5.02	1.47	0.916				
Information quality	IQ1	5.76	1.30	0.907	0.832	0.798	0.908	0.525
	IQ2	5.27	1.48	0.917				
System quality	SQ1	5.90	1.30	0.956	0.909	0.950	0.968	0.478
	SQ2	5.78	1.28	0.947				
	SQ3	5.83	1.30	0.958				
Enjoyment	ENJ1	4.51	1.68	0.954	0.907	0.949	0.967	0.312
	ENJ2	4.41	1.66	0.957				
	ENJ3	4.79	1.62	0.946				
Usefulness	US1	5.38	1.46	0.947	0.898	0.943	0.963	0.520
	US2	5.36	1.45	0.955				
	US3	5.48	1.48	0.940				
Satisfaction	SAT1	5.40	1.37	0.979	0.959	0.957	0.979	0.741
	SAT2	5.32	1.46	0.979				
Security self-efficacy	SE1	5.74	1.25	0.968	0.935	0.965	0.977	0.426
	SE2	5.75	1.29	0.960				
	SE3	5.77	1.24	0.973				

Note: CR: Composite reliability; AVE: Average variance extracted; N/A: Not applicable.

Table 4
Fornell–Larcker test.

	1	2	3	4	5	6	7	8	9	10
1. Challenges	**0.945**									
2. Feedback	0.218	**0.944**								
3. Clear goals	0.246	0.730	**0.962**							
4. Narrative	0.392	0.580	0.616	**0.936**						
5. Information quality	0.351	0.619	0.668	0.768	**0.912**					
6. System quality	0.210	0.641	0.663	0.640	0.713	**0.954**				
7. Enjoyment	0.442	0.383	0.418	0.623	0.682	0.502	**0.952**			
8. Usefulness	0.449	0.488	0.517	0.646	0.726	0.606	0.650	**0.947**		
9. Satisfaction	0.405	0.557	0.622	0.758	0.819	0.674	0.756	0.765	**0.979**	
10. Self-efficacy	0.281	0.595	0.656	0.615	0.653	0.582	0.444	0.594	0.663	**0.967**

Note: The values on the diagonal are the square roots of the AVEs. Values below the diagonal are construct correlations.

Table 5
Formative measurement model results (second-order constructs).

Construct	**Items**	**Loading**	**t-value**	**Weight**	**t-value**	**VIF**
Gamification	Challenges	0.455	14.387	0.102	4.166	1.182
	Feedback	0.768	30.986	0.182	4.917	2.278
	Clear goals	0.818	41.086	0.273	7.458	2.438
	Narrative	0.941	105.465	0.627	20.768	1.899

Note: VIF: Variance inflation factor.

and H1c. Information quality (β = 0.409; t = 9.325), system quality (β = 0.171; t = 4.704) and enjoyment (β = 0.284; t = 8.490) were positively associated with perceived usefulness, supporting H2a, H2b and H2c. Similarly, information quality (β = 0.350; t = 9.847), system quality (β = 0.131; t = 4.520) and enjoyment (β = 0.296; t = 11.415) were positively related to satisfaction, supporting H3a, H3b and H3c. Perceived usefulness was shown to promote satisfaction (β = 0.239; t = 8.844), supporting H4. Finally, the findings demonstrated that perceived usefulness (β = 0.208; t = 5.179) and employee satisfaction with the e-training (β = 0.506; t = 12.954) increased employees' security self-efficacy, supporting H5 and H6. The only control variable with a significant impact on employees' security self-efficacy was the time elapsed since they last completed the e-training (β = − 0.046; t = 2.077); employees who had completed the e-training more recently showed higher security self-efficacy.

5. Study 2

Study 1 provided interesting insights into the employees' perceptions. Study 2 addressed the second research question by analysing, through objective measures (i.e. the employees' actual behaviours), the effectiveness of gamified information security and data protection e-training systems.

Table 6
Structural model results.

Hypotheses	β	t-value	Supported
H1a: Gamification →Information quality	0.813	60.098***	Yes
H1b Gamification →System quality	0.721	33.276***	Yes
H1c: Gamification →Enjoyment	0.620	31.265***	Yes
H2a: Information quality →Perceived usefulness	0.409	9.325***	Yes
H2b: System quality →Perceived usefulness	0.171	4.704***	Yes
H2c: Enjoyment →Perceived usefulness	0.284	8.490***	Yes
H3a: Information quality →Satisfaction	0.350	9.847***	Yes
H3b: System quality →Satisfaction	0.131	4.520***	Yes
H3c: Enjoyment →Satisfaction	0.296	11.415***	Yes
H4: Perceived usefulness →Satisfaction	0.239	8.844***	Yes
H5: Perceived usefulness →Security self-efficacy	0.208	5.179***	Yes
H6: Satisfaction →Security self-efficacy	0.506	12.954***	Yes
Control variables:			
Time elapsed →Security self-efficacy	−0.046	2.077**	
Work experience →Security self-efficacy	0.017	0.724	
Gender →Security self-efficacy	−0.011	0.433	
Age →Security self-efficacy	0.019	0.769	

Note: ***p < 0.01; **p < 0.05.

5.1. Methodology

5.1.1. Participants and procedure

The employees' responses to a phishing attack were chosen as the objectively auditable security behaviours. As previously noted, this is one of the most common types of cyberattack. The phishing campaign targeted the employees of the same large company examined in Study 1. All employees of the company, who have a company email address and, therefore, access to the company's IT systems, participated in the phishing campaign. The phishing campaign was launched three months after the survey was distributed, that is, in June 2021. As shown in Fig. 2, the campaign consisted of two phishing waves, with a period of five months between the first and second waves; in this intervening period, the employees completed a gamified e-training course with the same structure and design as the e-training analysed in Study 1 but, in this case, focused on the topic of phishing. The gamified e-training was mandatory for all employees.

The phishing campaign was designed, in collaboration with the organisation, by a well-known international provider of information security awareness training. The provider offers a wide range of scenarios, which are categorised and grouped into three levels of difficulty (beginner, advanced and expert). To ensure comparability between the two waves, the same level was selected for both (i.e. advanced). The phishing email used in the first wave pretended to be a notification that a colleague had shared a Word document via Microsoft Teams, which was available for download. In the second wave, the phishing email tried to capture the users' attention by telling them about a new search engine, supposedly developed by the company as part of a joint industry project, through which employees could view the personal information held on them on the Internet. Both scenarios included a hyperlink and endeavoured to trick the user into clicking the link, which would lead to a fake website. This website then asked the user to enter their username and password to access the document sent in the first wave and the information stored on the Internet in the second wave. In addition, both scenarios included classic phishing cues (e.g. impersonal speech, importance and urgency, a non-company sender address and a link to an unsecured website), which are often important alerts in phishing email detection (Canham et al., 2022).

In particular, some 13,452 phishing emails were sent in the first wave and 13,714 in the second. Thus, most of the company's employees received phishing mails. The phishing scenario for the first wave was identical in all cases. A video of the CEO explaining the phishing test, and the importance of identifying fake emails and acting correctly, was shown to those employees who clicked on the link. Three days after the first wave all employees, including those who acted correctly during the test, received a company newsletter showing the video and the results of the phishing campaign. As mentioned before, the scenario in the second phishing wave was different, but the difficulty level and structure were the same as in the first wave to ensure comparability. In the second phishing wave a video of the CISO, also explaining the phishing test and the importance of identifying fake emails and acting correctly, was shown to the employees who clicked on the link. Again, three days after the phishing emails were sent, employees received a communication with the CISO's video and the campaign results.

5.1.2. Measures

After both waves, the number of emails opened, links clicked, usernames/passwords submitted by employees (after clicking on the link in the fake email employees were asked to introduce some personal data, such as a username and password) and the number of phishing emails reported to the company's IT service desk, were recorded. While opening the phishing email, clicking on the link in the fake email and submitting one's credentials are considered negative actions, reporting the phishing email to the company's IT service desk is the desired behaviour. The employees had two ways of reporting the suspicious email as a potential phishing attack. The first was to forward it to the information security team's mailbox, and the second was to push a "Phishing Report Button" built into Outlook, which automatically forwarded it to the security team. Both options automatically create a support case in the company's IT ticketing system, and all tickets are centrally processed, monitored, tracked and evaluated.

For security and confidentiality reasons, only the variation in the click rate percentage (i.e. the percentage of employees who clicked on the phishing link inside the email), and in the percentage of phishing emails reported to supervisors, can be identified in this study.

5.2. Results

To address the research question, the variation in the click rate percentage and the percentage of phishing emails reported to

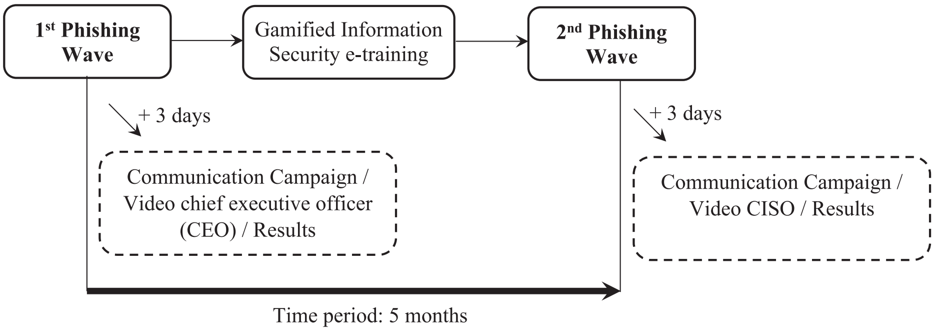
1st Phishing Wave
Gamified Information Security e-training
2nd Phishing Wave
+ 3 days
Communication Campaign / Video chief executive officer (CEO) / Results
+ 3 days
Communication Campaign / Video CISO / Results
Time period: 5 months

Fig. 2. Timeline of phishing campaign.

supervisors were analysed. The variation in the click rate percentage significantly decreased from the first wave to the second wave, by which time the employees had completed the gamified e-training; the total percentage reduction between the first and second waves was 50.2 %. As previously noted, the click rate itself cannot be reported due to security and confidentiality reasons. The phishing campaign also measured how many employees reported the suspicious phishing email to their supervisor or the information security team, which is the desired behaviour. In this case, the reporting rate increased by 70 % between the first and second waves, after completion of the gamified e-training.

6. Discussion

Drawing on the IS success literature and gamification theory, this study provides empirical evidence of the potential of gamification to increase the success of information security and data protection e-training systems and employee security self-efficacy. In particular, the results show that gamification positively influences critical dimensions of IS success: information quality and system quality, which in turn impact the perceived usefulness and satisfaction with e-training systems. Employee enjoyment is also influenced by gamification and, as with information and system quality, it impacts perceived usefulness and satisfaction. The findings also show that perceived usefulness enhances employee satisfaction, and both variables improve employee perceptions of security self-efficacy. This research further shows that gamified e-training systems enhance employees' information security-related behaviours. Specifically, after completing the gamified e-training, in the phishing attack scenario, the percentage of clicks on the fake link decreased significantly and the percentage of phishing emails reported to the supervisor increased. These findings are discussed in more detail below.

Study 1 explored employees' subjective perceptions of a German multinational company. As expected, the results confirmed that gamification improves the information quality delivered through the e-training and the e-training system quality. These findings are in line with previous research that found that gamification is a powerful tool for transmitting information and facilitating information system navigation (Rodrigues et al., 2017). In addition, the findings suggested that gamification increases participants' enjoyment of the training experience. This result is consistent with previous literature that found that gamification influences the hedonic value (Högberg et al., 2019) and enjoyment (Gerdenitsch et al., 2020; Zhang et al., 2021) of an activity. Thus, including game elements in online training systems helps employees to better understand the content of training sessions, perceive them as easier to use and enjoy the training experience more.

The findings also showed that information quality and system quality enhance employees' perceptions of the usefulness of e-training systems. Previous studies in the online learning context have also demonstrated that information quality (e.g. Al-Fraihat et al., 2020; Lwoga, 2014), as well as system quality (e.g. Al-Fraihat et al., 2020) and perceived ease of use (Lee et al., 2019; Manis & Choi, 2019) increase perceived usefulness of the learning system. According to our predictions, employees' enjoyment of the e-training system increased perceptions of usefulness. This result is in line with prior literature in contexts such as education (Abdullah et al., 2016), mobile technologies (Alalwan et al., 2018), banking technologies (de Oliveira et al., 2019), augmented/virtual reality technologies (Holdack et al., 2022; Lee et al., 2019; Manis & Choi, 2019) or distance learning (Rizun & Strzelecki, 2020; Syahruddin et al., 2021).

Information quality and system quality increased employees' satisfaction with e-training systems. These findings are consistent with the IS success literature (DeLone & McLean, 1992, 2003; Seddon, 1997; Seddon & Kiew, 1996) and prior research that found that providing interesting and understandable content (Al-Fraihat et al., 2020; Cidral et al., 2018; Martins et al., 2019) and accessing user-friendly and well-structured systems increase learner satisfaction (Aparicio et al., 2019; Cidral et al., 2018; Marjanovic et al., 2016; Martins et al., 2019). Furthermore, as prior research has demonstrated that feelings of enjoyment while interacting with a technology enhance user satisfaction (Muñoz-Carril et al., 2021; Silic et al., 2020; Yousaf et al., 2021), our findings confirmed that enjoyment increases employee satisfaction with e-training systems. Perceived usefulness, in turn, was shown to generate higher satisfaction, which aligns with the IS success literature (Chen, 2010; Seddon & Kiew, 1996).

Finally, the results demonstrated that perceived usefulness and satisfaction lead to higher security self-efficacy. In other words, these factors increase employees' perceptions of being able to comply with security requirements and cope with security threats. These results are consistent with previous e-learning systems literature, which supports the role of usefulness and satisfaction in providing benefits to learners and in increasing their knowledge (Al-Fraihat et al., 2020).

Study 2 went beyond employee perceptions and analysed, through objective measures, their actual information security behaviours. In particular, employee responses to a phishing attack were explored. Negative behaviours, such as clicking on the phishing email link, and positive behaviours, such as reporting the email to the company's IT service desk, were measured. The results from the phishing campaign showed that employees improved their information security behaviours after completing gamified e-training. In particular, the click rate percentage for the phishing email link decreased significantly from the first phishing wave to the second, which is consistent with previous literature on information security awareness (Silic & Lowry, 2020). Moreover, the reporting rate increased between the first and the second wave. Therefore, the results showed that employee training not only reduces the number of victims of phishing attacks but also promotes positive reactions to those attacks (Canham et al., 2022). This response is especially important as it can alert the organisation to a potential threat.

6.1. Theoretical contributions

This study makes a number of theoretical contributions. Although gamification is a strategy used in different contexts, it is relatively underrepresented in the IS literature (Koivisto & Hamari, 2019) and few studies have empirically analysed its impact on information security education and training (Chen et al., 2023; Silic & Lowry, 2020). Likewise, although the IS success literature provides a comprehensive framework for evaluating the success of gamified systems, this theoretical framework has seldom been used (Aparicio et al., 2019). Drawing on Seddon's (1997) model, this study contributes to the gamification literature (Koivisto & Hamari, 2019; Rapp et al., 2019), in general, and the security gamification literature (Chen et al., 2023; Silic & Lowry, 2020), in particular, by demonstrating that gamification increases e-training systems success and enhances employee information security self-efficacy. The study also contributes to the IS literature. In a recent IS success literature review, Jeyaraj (2020) highlighted that previous studies in the field have focused on IS success variables and that the antecedents of IS success remain unexplored. Therefore, the present study extends the IS success literature by analysing the use of gamification as a driver of IS success. The results also support the relationships proposed between the different measures of IS success, reinforcing the importance of these variables.

This research also overcomes some of the methodological shortcomings related to data-gathering. Unlike many previous studies, which use student samples, the present study analyses the perceptions of 1,178 employees of a German multinational corporation who had previously completed gamified e-training courses in information security and data protection. In addition, while previous studies have emphasised the need to objectively analyse employee security behaviours (van Steen & Deeleman, 2021), research into the effect of gamification on both employees' perceptions and actual behaviours is uncommon. Therefore, a further contribution of this paper is the analysis of both employees' subjective perceptions and their actual behaviours to investigate the effectiveness of gamified information security and data protection e-training systems.

6.2. Practical implications

This study also provides a number of practical implications for cyber professionals. Cyberattacks were reported as the biggest business risk in 2022 (Statista, 2022) and 95 % of all cyber security issues are related to human error (World Economic Forum, 2022). The results of our study can contribute to mitigating cyber security risks, as they show that gamified e-training increases employees' perceptions of security self-efficacy and improves information security behaviours. Although investments in technological solutions and security products to reduce the risk of cyberattacks are needed (Kweon et al., 2021), the findings of this study highlight the importance of using gamified e-training systems to improve employee perceptions and behaviours. The use of this innovative strategy can motivate and engage employees more effectively than traditional methods.

Our results also show that employee perceptions and responses to a phishing attack improved after completing gamified e-training that included the following game elements: challenges, clearly defined learning goals, continuous feedback and narrative with real and animated videos. Therefore, the research provides guidelines to design and develop security awareness courses that effectively increase self-efficacy in information security and data protection. First, it is important that e-training systems include goals that clearly explain the instructions for successfully completing the training course. Training goals should be outlined at the beginning of the course to explain its importance, the structure of the course (i.e. number of sections), the tasks they have to complete, etc. It is important that the employees perceive that, with proper instruction, they can successfully complete their e-training. Challenges or quests are also important game elements in e-training systems. These should be implemented in the form of problem-solving exercises that provide employees with a sense of achievement (e.g. puzzles and drag-and-drop activities). They are important interactive elements that require active employee participation. Moreover, challenges should be demanding tasks with appropriate levels of difficulty, and the learners should also understand that resolving them requires effort. Challenges should be set at appropriate levels of difficulty. The systems should also provide continuous and concrete feedback so that employees know how are performing. Points, levels and progress bars can be used to provide learners with immediate feedback about their performance and progress in the training course. For instance, progress bars may show the number of chapters successfully completed. Feedback in the training course may also take the format of dialogues and/or instant messages that reinforce good performance and provide advice about how it might be improved. Finally, instead of presenting the course content using slideshows or webpages, designers and developers might also include animated and real videos that tell a meaningful and ongoing story that immerses participants in the training. The use of stories and narrative add context and depth to the learning experience. Consequently, it is more likely that employees will recall the information over a longer period. As such, the training might use videos showing real-world examples of potential breaches and threats and explaining the key role of employees in ensuring information security in the company.

Other game elements not included in the e-training analysed, such as badges and achievements, avatars or levels, could also be very valuable to enhance e-training system success and, hence, increase employee perceptions of having the ability to perform appropriate information security behaviours.

6.3. Limitations and future research directions.

First, the data were collected using a self-administered questionnaire in a cross-sectional study. Future research might use longitudinal data to analyse gamification effectiveness over time. Second, this research investigates both employees' perceptions of gamified e-training systems (Study 1) and their actual security behaviours (Study 2). However, due to data privacy issues, it was not possible to track the employees' perceptions and subsequent actual behaviours. In addition, for security and confidentiality reasons, in Study 2 it was only possible to report variations in the click rate percentage and the percentage of phishing emails reported. Third, although the study was carried out in an actual organisation with a real gamified security e-training system, analysing only one organisation limits the generalisability of the results. Finally, the phishing campaign was conducted without a control group, so future research should replicate the study comparing the results of employees who have undergone gamified e-training with those who have not.

CRediT authorship contribution statement

Paula Bitrián: Writing – original draft, Validation, Supervision, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization. **Isabel Buil:** Data curation, Conceptualization, Formal analysis, Funding acquisition, Investigation, Methodology, Supervision, Validation, Writing – original draft. **Sara Catalán:** Writing – original draft, Validation, Supervision, Methodology, Investigation, Funding acquisition, Formal analysis, Conceptualization, Data curation. **Dominik Merli:** Writing – original draft, Validation, Supervision, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This study was supported by the Spanish Ministry of Economy, Industry and Competitiveness and the European Regional Development Fund (project ECO2017-82103-P), the Spanish Ministry of Universities (pre-doctoral grant FPU19/01471), and the Government of Aragon (GENERES Group S54_23R) co-financed by FEDER 2014-2020 'Building Europe from Aragon'. Paula Bitrián would also like to thank the financial support received from the Universidad de Zaragoza, Fundación Bancaria Ibercaja y Fundación CAI (Ref: CH 25/20) (Programa Ibercaja-CAI de Estancias de Investigación).

Appendix A. . Constructs, items and sources

Construct and source	Items
GamificationSilic and Lowry (2020); Fu et al. (2009); Green and Brock (2000)	***Challenges*** **CH1.** Completing the different practical exercises (such as puzzles) is challenging **CH2.** The different practical exercises of the e-training are demanding ***Feedback***

(*continued on next page*)

(*continued*)

Construct and source	Items
	FE1. While I am completing the e-training, I receive feedback on the progress made (such as chapters completed)
	FE2. While I am completing the e-training, I receive immediate information on my success (or failure)
	FE3. While I am completing the e-training, I receive information on my score
	Clear goals
	GO1. Overall learning goals are presented at the beginning of the e-training
	GO2. Overall learning goals are clear to me
	Narrative context
	NAR1. While I was watching the videos, I could easily picture the events in them taking place
	NAR2. I could visualise myself in the events described in the videos
	NAR3. I was mentally involved in the videos while watching them
Information quality Aparicio et al. (2019)	**IQ1.** The content provided by the e-training is understandable
	IQ2 The content provided by the e-training is interesting
System quality Davis (1989); Aparicio et al. (2019)	**SQ1.** The e-training is easy to use
	SQ2. The e-training is well structured
	SQ3. The e-training is easy to interact with
EnjoymentVenkatesh (2000)	**ENJ1.** I have fun completing the e-training
	ENJ2. I find the e-training enjoyable
	ENJ3. I find the e-training pleasant
UsefulnessDavis (1989)	**US1.** The e-training improves my information security and data protection behaviour
	US2. The e-training enables me to better react to potential cyber security threats
	US3. The e-training is useful
SatisfactionKettanurak et al. (2001)	**SAT1.** Overall, I am very satisfied with the e-training
	SAT2. Overall, I have had a very positive learning experience
Security self-efficacy Silic and Lowry (2020)	**SE1.** I am confident that I can perform proper information security behaviours
	SE2. I can protect my computer by following proper information security behaviours
	SE3. I am able to perform proper information security behaviours

References

Abdullah, F., Ward, R., & Ahmed, E. (2016). Investigating the influence of the most commonly used external variables of TAM on students' Perceived Ease of Use (PEOU) and Perceived Usefulness (PU) of e-portfolios. *Computers in Human Behavior, 63*, 75–90. https://doi.org/10.1016/j.chb.2016.05.014

Abraham, S., & Chengalur-Smith, I. S. (2019). Evaluating the effectiveness of learner controlled information security training. *Computers and Security, 87*, Article 101586. https://doi.org/10.1016/j.cose.2019.101586

Adams, M., & Makramalla, M. (2015). Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. *Technology Innovation. Management Review, 5*(1). https://doi.org/10.22215/timreview/861

Al-Fraihat, D., Joy, M., Masa'deh, R., & Sinclair, J. (2020). Evaluating E-learning systems success: An empirical study. *Computers in Human Behavior, 102*, 67–86. https://doi.org/10.1016/j.chb.2019.08.004

Alalwan, A. A., Baabdullah, A. M., Rana, N. P., Tamilmani, K., & Dwivedi, Y. K. (2018). Examining adoption of mobile internet in Saudi Arabia: Extending TAM with perceived enjoyment, innovativeness and trust. *Technology in Society, 55*, 100–110. https://doi.org/10.1016/j.techsoc.2018.06.007

Aldalur, I., & Perez, A. (2023). Gamification and discovery learning: Motivating and involving students in the learning process. *Heliyon, 9*(1). https://doi.org/10.1016/j.heliyon.2023.e13135

Alqahtani, H., & Kavakli-Thorne, M. (2020). Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). *Information, 11*(2), 121. https://doi.org/10.3390/info11020121

Andersson, A., Hedström, K., & Karlsson, F. (2022). Standardizing information security – a structurational analysis. *Information and Management, 59*(3), Article 103623. https://doi.org/10.1016/j.im.2022.103623

Aparicio, M., Bacao, F., & Oliveira, T. (2016). Cultural impacts on e-learning systems' success. *Internet and Higher Education, 31*, 58–70. https://doi.org/10.1016/j.iheduc.2016.06.003

Aparicio, M., Oliveira, T., Bacao, F., & Painho, M. (2019). Gamification: A key determinant of massive open online course (MOOC) success. *Information and Management, 56*(1), 39–54. https://doi.org/10.1016/j.im.2018.06.003

Bai, S., Hew, K. F., & Huang, B. (2020). Does gamification improve student learning outcome? Evidence from a meta-analysis and synthesis of qualitative data in educational contexts. *Educational Research Review, 30*, Article 100322. https://doi.org/10.1016/j.edurev.2020.100322

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191–215. https://doi.org/10.1037/0033-295X.84.2.191

Banfield, J., & Wilkerson, B. (2014). Increasing Student Intrinsic Motivation And Self-Efficacy Through Gamification Pedagogy. *Contemporary Issues in Education Research (CIER), 7*(4), 291–298. https://doi.org/10.19030/cier.v7i4.8843

Baxter, R. J., Holderness, D. K., & Wood, D. A. (2016). Applying basic gamification techniques to it compliance training: Evidence from the lab and field. *Journal of Information Systems, 30*(3), 119–133. https://doi.org/10.2308/isys-51341

Behl, A., Jayawardena, N., Pereira, V., Islam, N., Del Giudice, M., & Choudrie, J. (2022a). Gamification and e-learning for young learners: A systematic literature review, bibliometric analysis, and future research agenda. *Technological Forecasting and Social Change, 176*, Article 121445. https://doi.org/10.1016/j.techfore.2021.121445

Behl, A., Pereira, V., Sindhwani, R., Bhardwaj, S., Papa, A., & Hassan, Y. (2022b). Improving Inclusivity of Digitalization for Employees in Emerging Countries Using Gamification. *IEEE Transactions on Engineering Management*. https://doi.org/10.1109/TEM.2022.3216553

Behl, A., Jayawardena, N., Ishizaka, A., Gupta, M., & Shankar, A. (2022c). Gamification and gigification: A multidimensional theoretical approach. *Journal of Business Research, 139*, 1378–1393. https://doi.org/10.1016/j.jbusres.2021.09.023

Behl, A., Pereira, V., Jayawardena, N., Nigam, A., & Mangla, S. (2023). Gamification as an innovation: A tool to improve organizational marketing performance and sustainability of international firms. *International Marketing Review*. https://doi.org/10.1108/IMR-05-2022-0113

Bellon, L. (2020). Cisco Umbrella's Top 10 Cybersecurity Tips. Retrieved from https://umbrella.cisco.com/blog/cisco-umbrella-top-10-cybersecurity-tips.

Bioglio, L., Capecchi, S., Peiretti, F., Sayed, D., Torasso, A., & Pensa, R. G. (2019). A Social Network Simulation Game to Raise Awareness of Privacy among School Children. *IEEE Transactions on Learning Technologies, 12*(4), 456–469. https://doi.org/10.1109/TLT.2018.2881193

Boopathi, K., Sreejith, S., & Bithin, A. (2015). Learning cyber security through gamification. *Indian Journal of Science and Technology, 8*(7), 642–649. https://doi.org/10.17485/ijst/2015/v8i7/67760

Bossman, A., & Agyei, S. K. (2022). Technology and instructor dimensions, e-learning satisfaction, and academic performance of distance students in Ghana. *Heliyon, 8*(4), e09200.

Canham, M., Posey, C., & Constantino, M. (2022). Phish Derby: Shoring the Human Shield Through Gamified Phishing Attacks. *Frontiers in Education, 6*, 536. https://doi.org/10.3389/feduc.2021.807277

Carmines, E. G., & Zeller, R. A. (1979). Reliability and validity assessment. *Sage*. Publications.

Chen, H., Zhang, Y., Zhang, S., & Lyu, T. (2023). Exploring the role of gamified information security education systems on information security awareness and protection behavioral intention. *Education and Information Technologies, 1–34*. https://doi.org/10.1007/s10639-023-11771-z

Cidral, W. A., Oliveira, T., Di Felice, M., & Aparicio, M. (2018). E-learning success determinants: Brazilian empirical study. *Computers and Education, 122*, 273–290. https://doi.org/10.1016/j.compedu.2017.12.001

Costa, J. A. F. (2020). Data protection in international trade law. *Data protection in the internet*, 479–517.

Csikszentmihalyi, M. (1975). *Beyond Boredom and Anxiety*. San Francisco: JosseyBass.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly, 13*(3), 319–340.

de Almeida, J. L. F., & dos Santos Machado, L. (2021). Design requirements for educational serious games with focus on player enjoyment. *Entertainment Computing, 38*, Article 100413. https://doi.org/10.1016/j.entcom.2021.100413

De Oliveira, F., Junior, W., Hoffmann, C., Gattermann, M., & Cunha, P. (2019). A meta-analytical study of technological acceptance in banking contexts. *International Journal of Bank Marketing, 37*(3), 755–774. https://doi.org/10.1108/IJBM-04-2018-0110

DeLone, W., & McLean, E. (1992). Information systems success: The quest for the dependent variable. *Information Systems Research, 3*(1), 60–95.

DeLone, W., & McLean, E. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. *Journal of Management Information Systems, 19* (4), 9–30.

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From Game Design Elements to Gamefulness: Defining "Gamification". *MindTrek*, 9–15.

Dincelli, E., & Chengalur-Smith, I. S. (2020). Choose your own training adventure: Designing a gamified SETA artefact for improving information security and privacy through interactive storytelling. *European Journal of Information Systems, 29*(6), 669–687. https://doi.org/10.1080/0960085X.2020.1797546

Donovan, E., Guzman, I. R., Adya, M., & Wang, W. (2018). A Cloud Update of the DeLone and McLean Model of Information Systems. *Journal of Information Technology Management, 29*(3), 23–34.

Enisa (2017). *Phishing on the rise*. Retrieved from https://www.enisa.europa.eu/publications/info-notes/phishing-on-the-rise.

ENISA (2023). *ENISA Threat Landscape 2023. July 2022 to June 2023*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023/@@download/fullReport.

Eraslan Yalcin, M., & Kutlu, B. (2019). Examination of students' acceptance of and intention to use learning management systems using extended TAM. *British Journal of Educational Technology, 50*(5), 2414–2432. https://doi.org/10.1111/bjet.12798

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50.

Fu, F. L., Su, R. C., & Yu, S. C. (2009). EGameFlow: A scale to measure learners' enjoyment of e-learning games. *Computers and Education, 52*(1), 101–112. https://doi.org/10.1016/j.compedu.2008.07.004

García-Jurado, A., Torres-Jiménez, M., Leal-Rodríguez, A. L., & Castro-González, P. (2021). Does gamification engage users in online shopping? *Electronic Commerce Research and Applications, 48*, Article 101076. https://doi.org/10.1016/j.elerap.2021.101076

Gerdenitsch, C., Sellitsch, D., Besser, M., Burger, S., Stegmann, C., Tscheligi, M., & Kriglstein, S. (2020). Work gamification: Effects on enjoyment, productivity and the role of leadership. *Electronic Commerce Research and Applications, 43*, Article 100994. https://doi.org/10.1016/j.elerap.2020.100994

Ghazvini, A., & Shukur, Z. (2018). A serious game for healthcare industry: Information security awareness training program for Hospital Universiti Kebangsaan Malaysia. *International Journal of Advanced Computer Science and Applications, 9*(9), 236–245. https://doi.org/10.14569/ijacsa.2018.090932

Goel, S., Williams, K. J., Huang, J., & Warkentin, M. (2021). Can financial incentives help with the struggle for security policy compliance? *Information & management, 58*(4), Article 103447. https://doi.org/10.1016/j.im.2021.103447

Green, M. C., & Brock, T. C. (2000). The role of transportation in the persuasiveness of public narratives. *Journal of Personality and Social Psychology, 79*(5), 701–721. https://doi.org/10.1037/0022-3514.79.5.701

Ha, I., Yoon, Y., & Choi, M. (2007). Determinants of adoption of mobile games under mobile broadband wireless access environment. *Information & management, 44*(3), 276–286. https://doi.org/10.1016/j.im.2007.01.001

Hair, J., Hollingsworth, C. L., Randolph, A. B., & Chong, A. Y. L. (2017a). An updated and expanded assessment of PLS-SEM in information systems research. *Industrial management & data systems, 117*(3), 442–458. https://doi.org/10.1108/IMDS-04-2016-0130

Hair, J. F., Hult, G. T., Ringle, C. M., & Sarstedt, M. (2017b). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) (Second)*. Los Angeles: SAGE.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a siler bullet. *Journal of Marketing Theory and Practice, 19*(2), 139–152.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Gundergan, P. (2018). *Advanced Issues in Partial Least Squares Structural Equation Modeling*. Los Angeles: SAGE.

Hamari, J., Koivisto, J., & Sarsa, H. (2014). Does gamification work? - A literature review of empirical studies on gamification. *Proceedings of the HICSS 2013 Conference. Washington*, DC, 3025–3034. doi: 10.1109/HICSS.2014.377.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers and Security, 95*, Article 101827. https://doi.org/10.1016/j.cose.2020.101827

Hendrix, M., Al-sherbaz, A., & Bloom, V. (2016). Game Based Cyber Security Training: Are Serious Games suitable for cyber security training? *International Journal of Serious Games, 3*(1).

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Högberg, J., Ramberg, M. O., Gustafsson, A., & Wästlund, E. (2019). Creating brand engagement through in-store gamified customer experiences. *Journal of Retailing and Consumer Services, 50*, 122–130. https://doi.org/10.1016/j.jretconser.2019.05.006

Holdack, E., Lurie-Stoyanov, K., & Fromme, H. F. (2022). The role of perceived enjoyment and perceived informativeness in assessing the acceptance of AR wearables. *Journal of Retailing and Consumer Services, 102259*. https://doi.org/10.1016/j.jretconser.2020.102259

Hsu, C. L., & Lin, J. C. C. (2016). Effect of perceived value and social influences on mobile app stickiness and in-app purchase intention. *Technological Forecasting and Social Change, 108*, 42–53. https://doi.org/10.1016/j.techfore.2016.04.012

Hu, L., & Bentler, P. M. (1998). Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification. *Psychological Methods, 3*(4), 424–453. https://doi.org/10.1037//1082-989x.3.4.424

Ibm. (2023). Cost of a Data Breach Report 2023. Retrieved from https://www.ibm.com/security/data-breach.

Iseni, A. (2021). Top 5 Types of Security Threats to Look Out for in 2022. Retrieved from https://pecb.com/article/top-5-types-of-security-threats-to-look-out-for-in-2022.

Jayawardena, N. S., Ross, M., Quach, S., Behl, A., & Gupta, M. (2021). Effective online engagement strategies through gamification: A systematic literature review and a future research agenda. *Journal of Global Information Management, 30*(5), 1–25. https://doi.org/10.4018/JGIM.290370

Jeyaraj, A. (2020). DeLone & McLean models of information system success: Critical meta-review and research directions. *International Journal of Information Management, 54*, Article 102139. https://doi.org/10.1016/j.ijinfomgt.2020.102139

Joo, Y. J., So, H. J., & Kim, N. H. (2018). Examination of relationships among students' self-determination, technology acceptance, satisfaction, and continuance intention to use K-MOOCs. *Computers and Education, 122*, 260–272. https://doi.org/10.1016/j.compedu.2018.01.003

Kapp, K. M. (2012). *The gamification of learning and instruction: Game-based methods and strategies for training and education*. John Wiley & Sons.

Karagiannis, S., & Magkos, E. (2020). Adapting CTF challenges into virtual cybersecurity learning environments. *Information and Computer Security, 29*(1), 105–132. https://doi.org/10.1108/ICS-04-2019-0050

Kettanurak, V. N., Ramamurthy, K., & Haseman, W. D. (2001). User attitude as a mediator of learning performance improvement in an interactive multimedia environment: An empirical investigation of the degree of interactivity and learning styles. *International Journal of Human-Computer Studies, 54*(4), 541–583. https://doi.org/10.1006/ijhc.2001.0457

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers and Security, 106*, Article 102267. https://doi.org/10.1016/j.cose.2021.102267

Kim, S. (2021). How a company's gamification strategy influences corporate learning: A study based on gamified MSLP (Mobile social learning platform). *Telematics and Informatics, 57*, Article 101505. https://doi.org/10.1016/j.tele.2020.101505

Kock, N. (2015). Common Method Bias in PLS-SEM: A full collinearity assessment approach. *International Journal of E-Collaboration, 11*(4), 1–10.

Koivisto, J., & Hamari, J. (2019). The rise of motivational information systems: A review of gamification research. *International Journal of Information Management, 45*, 191–210. https://doi.org/10.1016/j.ijinfomgt.2018.10.013

Krath, J., Schürmann, L., & von Korflesch, H. F. O. (2021). Revealing the theoretical basis of gamification: A systematic review and analysis of theory in research on gamification, serious games and game-based learning. *Computers in Human Behavior, 125*, Article 106963. https://doi.org/10.1016/j.chb.2021.106963

Küpper, D. M., Klein, K., & Völckner, F. (2021). Gamifying employer branding: An integrating framework and research propositions for a new HRM approach in the digitized economy. *Human Resource Management Review, 31*(1), Article 100686. https://doi.org/10.1016/j.hrmr.2019.04.002

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence. *Information Systems Frontiers, 23*(2), 361–373. https://doi.org/10.1007/s10796-019-09977-z

Laine, T. H., & Lindberg, R. S. N. (2020). Designing Engaging Games for Education: A Systematic Literature Review on Game Motivators and Design Principles. *IEEE Transactions on Learning Technologies, 13*(4), 804–821. https://doi.org/10.1109/TLT.2020.3018503

Landers, R. N. (2014). Developing a Theory of Gamified Learning: Linking Serious Games and Gamification of Learning. *Simulation and Gaming, 45*(6), 752–768. https://doi.org/10.1177/1046878114563660

Lee, S., & Kim, D. Y. (2018). The effect of hedonic and utilitarian values on satisfaction and loyalty of Airbnb users. *International Journal of Contemporary Hospitality Management, 30*(3), 1332–1351. https://doi.org/10.1108/IJCHM-09-2016-0504

Lee, J., Kim, J., & Choi, J. Y. (2019). The adoption of virtual reality devices: The technology acceptance model integrating enjoyment, social interaction, and strength of the social ties. *Telematics and Informatics, 39*, 37–48. https://doi.org/10.1016/j.tele.2018.12.006

Luh, R., Temper, M., Tjoa, S., Schrittwieser, S., & Janicke, H. (2020). PenQuest: A gamified attacker/defender meta model for cyber security assessment and education. *Journal of Computer Virology and Hacking Techniques, 16*(1), 19–61. https://doi.org/10.1007/s11416-019-00342-x

Lwoga, E. (2014). Critical success factors for adoption of web-based learning management systems in Tanzania. *International Journal of Education and Development Using Information and Communication Technology, 10*(1), 4–21.

Manis, K. T., & Choi, D. (2019). The virtual reality hardware acceptance model (VR-HAM): Extending and individuating the technology acceptance model (TAM) for virtual reality hardware. *Journal of Business Research, 100*, 503–513. https://doi.org/10.1016/j.jbusres.2018.10.021

Marjanovic, U., Delić, M., & Lalic, B. (2016). Developing a model to assess the success of e-learning systems: Evidence from a manufacturing company in transitional economy. *Information Systems and E-Business Management, 14*(2), 253–272. https://doi.org/10.1007/s10257-015-0282-7

Martins, J., Branco, F., Gonçalves, R., Au-Yong-Oliveira, M., Oliveira, T., Naranjo-Zolotov, M., & Cruz-Jesus, F. (2019). Assessing the success behind the use of education management information systems in higher education. *Telematics and Informatics, 38*, 182–193. https://doi.org/10.1016/j.tele.2018.10.001

Mulcahy, R., Russell-Bennett, R., & Iacobucci, D. (2020). Designing gamified apps for sustainable consumption: A field study. *Journal of Business Research, 106*, 377–387. https://doi.org/10.1016/j.jbusres.2018.10.026

Muñoz-Carril, P. C., Hernández-Sellés, N., Fuentes-Abeledo, E. J., & González-Sanmamed, M. (2021). Factors influencing students' perceived impact of learning and satisfaction in Computer Supported Collaborative Learning. *Computers and Education, 174*, Article 104310. https://doi.org/10.1016/j.compedu.2021.104310

Ng, B. Y., Kankanhalli, A., Xu, Y., & (Calvin). (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815–825. https://doi.org/10.1016/j.dss.2008.11.010

Pereira, V., Behl, A., Jayawardena, N., Laker, B., Dwivedi, Y. K., & Bhardwaj, S. (2022). The art of gamifying digital gig workers: A theoretical assessment of evaluating engagement and motivation. *Production Planning & Control, 1–17*. https://doi.org/10.1080/09537287.2022.2083524

Petrykina, Y., Schwartz-Chassidim, H., & Toch, E. (2021). Nudging users towards online safety using gamified environments. *Computers and Security, 108*, Article 102270. https://doi.org/10.1016/j.cose.2021.102270

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. *Journal of Applied Psychology, 88*(5), 879. https://doi.org/10.1037/0021-9010.88.5.879

Rapp, A., Hopfgartner, F., Hamari, J., Linehan, C., & Cena, F. (2019). Strengthening gamification studies: Current trends and future opportunities of gamification research. *International Journal of Human Computer Studies, 127*, 1–6. https://doi.org/10.1016/j.ijhcs.2018.11.007

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816–826. https://doi.org/10.1016/j.cose.2009.05.008

Ringle, C. M., Wende, S., & Becker, J. M. (2015). *SmartPLS 3*. Bönningsted, Germany: SmartPLS GmbH.

Rizun, M., & Strzelecki, A. (2020). Students' acceptance of the covid-19 impact on shifting higher education to distance learning in Poland. *International Journal of Environmental Research and Public Health, 17*(18), 6468. https://doi.org/10.3390/ijerph17186468

Rodrigues, L. F., Costa, C. J., & Oliveira, A. (2017). How does the web game design influence the behavior of e-banking users? *Computers in Human Behavior, 74*, 163–174. https://doi.org/10.1016/j.chb.2017.04.034

Rohan, R., Funilkul, S., Pal, D., & Chutimaskul, W. (2021). Understanding of Human Factors in Cybersecurity: A Systematic Literature Review. *In 2021 International Conference on Computational Performance Evaluation (ComPE)*, 133–140, IEEE. doi: 10.1109/ComPE53109.2021.9752358.

Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. *Information and Management, 59*(4), Article 103638. https://doi.org/10.1016/j.im.2022.103638

Seddon. (1997). A Respecification and Extension of the DeLone and McLean Model of IS Success. *Information Systems Research, 8*(3), 240–253.

Seddon, P., & Kiew, M.-Y. (1996). A partila test and development of delone and Mclean's model of IS success. *Australasian Journal of Information Systems, 4*(1).

Silic, M., & Lowry, P. B. (2020). Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance. *Journal of Management Information Systems, 37*(1), 129–161. https://doi.org/10.1080/07421222.2019.1705512

Silic, M., Marzi, G., Caputo, A., & Bal, P. M. (2020). The effects of a gamified human resource management system on job satisfaction and engagement. *Human Resource Management Journal, 30*(2), 260–277. https://doi.org/10.1111/1748-8583.12272

Statista (2022). *The Biggest Business Risks in 2022*. Retrieved from https://www.statista.com/chart/26631/most-relevant-business-risks-in-2022/.

Statista (2023a). Global number of breached data sets Q1 2020-Q1 2023. Retrieved from https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/.

Statista (2023b). Spending on information security solutions and services worldwide 2023 vs. 2030. Retrieved from https://www.statista.com/statistics/640141/worldwide-information-security-solutions-and-services-spending/.

Statista (2023c). *Most commonly reported cyber crime categories worldwide in 2022, by number of individuals affected*. Retrieved from https://www.statista.com/statistics/184083/commonly-reported-types-of-cyber-crime-global/.

Sun, P. C., Tsai, R. J., Finger, G., Chen, Y. Y., & Yeh, D. (2008). What drives a successful e-Learning? An empirical investigation of the critical factors influencing learner satisfaction. *Computers and Education, 50*(4), 1183–1202. https://doi.org/10.1016/j.compedu.2006.11.007

Sun, P. C., Cheng, H. K., & Finger, G. (2009). Critical functionalities of a successful e-learning system - An analysis from instructors' cognitive structure toward system usage. *Decision Support Systems, 48*(1), 293–302. https://doi.org/10.1016/j.dss.2009.08.007

Syahruddin, S., Mohd Yaakob, M. F., Rasyad, A., Widodo, A. W., Sukendro, S., Suwardi, S., Lani, A., Sari, L. P., Mansur, M., Razali, R., & Syam, A. (2021). Students' acceptance to distance learning during Covid-19: The role of geographical areas among Indonesian sports science students. *Heliyon, 7*(9), e08043.

Szymkowiak, A., & Jeganathan, K. (2022). Predicting user acceptance of peer-to-peer e-learning: An extension of the technology acceptance model. *British Journal of Educational Technology, 53*(6), 1993–2011. https://doi.org/10.1111/bjet.13229

Tamjidyamcholo, A., Baba, M. S. B., Tamjid, H., & Gholipour, R. (2013). Information security–Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language. *Computers & Education, 68*, 223–232. https://doi.org/10.1016/j.compedu.2013.05.010

Thornton, D., & Francia, G., III (2014). Gamification of Information Systems and Security Training: Issues and Case Studies. *Information Security Education Journal, 1*(1), 16–29.

van Steen, T., & Deeleman, J. R. A. (2021). Successful Gamification of Cybersecurity Training. *Cyberpsychology, Behavior, and Social Networking, 24*(9), 593–598. https://doi.org/10.1089/cyber.2020.0526

Vedadi, A., Warkentin, M., & Dennis, A. (2021). Herd behavior in information security decision-making. *Information & Management, 58*(8), Article 103526. https://doi.org/10.1016/j.im.2021.103526

Venkatesh, V. (2000). Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model. *Information Systems Research, 11*(4), 342–365.

Verizon (2023). *2023 Data Breach Investigations Report*. Retrieved from https://www.verizon.com/business/resources/reports/dbir/.

Wang, P., & Li, H. (2019). Understanding the antecedents and consequences of the perceived usefulness of travel review websites. *International Journal of Contemporary Hospitality Management, 31*(3), 1086–1103. https://doi.org/10.1108/IJCHM-06-2017-0380

Wang, Y. F., Hsu, Y. F., & Fang, K. (2022). The key elements of gamification in corporate training–The Delphi method. *Entertainment Computing, 40*, Article 100463. https://doi.org/10.1016/j.entcom.2021.100463

Wee, S. C., & Choong, W. W. (2019). Gamification: Predicting the effectiveness of variety game design elements to intrinsically motivate users' energy conservation behaviour. *Journal of Environmental Management, 233*, 97–106. https://doi.org/10.1016/j.jenvman.2018.11.127

Wlosinski, L. G. (2019). The Benefits of Information Security and Privacy Awareness Training Programs. *Retrieved from*. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/the-benefits-of-information-security-and-privacy-awareness-training-programs.

Wolfenden, B. (2019). Gamification as a winning cyber security strategy. *Computer Fraud and Security, 2019*(5), 9–12. https://doi.org/10.1016/S1361-3723(19)30052-1

World Economic Forum (2022). *The Global Risks Report 2022*. Retrieved from https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf.

Wu, T., Tien, K. Y., Hsu, W. C., & Wen, F. H. (2021). Assessing the effects of gamification on enhancing information security awareness knowledge. *Applied Sciences, 11*(19), 9266. https://doi.org/10.3390/app11199266

Wünderlich, N. V., Gustafsson, A., Hamari, J., Parvinen, P., & Haff, A. (2020). The great game of business: Advancing knowledge on gamification in business contexts. *Journal of Business Research, 106*, 273–276. https://doi.org/10.1016/j.jbusres.2019.10.062

Yamin, M. M., Katt, B., & Nowostawski, M. (2021). Serious games as a tool to model attack and defense scenarios for cyber-security exercises. *Computers and Security, 110*, Article 102450. https://doi.org/10.1016/j.cose.2021.102450

Yasin, A., Liu, L., Li, T., Fatima, R., & Jianmin, W. (2019). Improving software security awareness using a serious game. *IET Software, 13*(2), 159–169. https://doi.org/10.1049/iet-sen.2018.5095

Yasin, A., Liu, L., Li, T., Wang, J., & Zowghi, D. (2018). Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG). *Information and Software Technology, 95*, 179–200. https://doi.org/10.1016/j.infsof.2017.12.002

Yousaf, A., Mishra, A., Taheri, B., & Kesgin, M. (2021). A cross-country analysis of the determinants of customer recommendation intentions for over-the-top (OTT) platforms. *Information and Management, 58*(8), Article 103543. https://doi.org/10.1016/j.im.2021.103543

Zhang, L., Shao, Z., Li, X., & Feng, Y. (2021). Gamification and online impulse buying: The moderating effect of gender and age. *International Journal of Information Management, 61*, Article 102267. https://doi.org/10.1016/j.ijinfomgt.2020.102267

Dr Paula Bitrián is Assistant Professor in the Department of Marketing Management at the University of Zaragoza, Spain. She holds a PhD in Business Administration. Her research concentrates on the issue of gamification. Her work has been published in journals such as *Journal of Business Research, International Journal of Bank Marketing, The International Journal of Management Education* and *European Journal of Management and Business Economics.* Paula is a member of the research group Generés recognised by the Government of Aragón.

Dr Isabel Buil is Professor of Marketing in the Faculty of Business and Economics at the University of Zaragoza, Spain. Her research focuses on brand management, consumer behaviour and gamification strategies. Her work has been published in journals such as *Journal of Business Research, Journal of Advertising Research, Tourism Management,* and *Journal of Business Ethics.* Isabel is a member of the research group Generés recognised by the Government of Aragón.

Dr Sara Catalán is Associate Professor in the Department of Marketing Management at the University of Zaragoza, Spain. She holds a PhD in Business Administration. Her research interests include gamification strategies and consumer behaviour. Her work has been published in journals such as *Journal of Business Research, International Journal of Hospitality Management, Online Information Review, Computers & Education, British Journal of Educational Technology* and *Journal of Product and Brand Management*. Sara is a member of the research group Generés.

Dr Dominik Merli is Professor for IT Security in the Faculty of Computer Science at Augsburg University of Applied Sciences and heads the Institute for innovative Safety and Security (HSA_innos). His research focuses on cyber security technologies and processes. His work has been published in proceedings of conference such as the USENIX Workshop on Offensive Technologies, the International Symposium for ICS & SCADA Cyber Security Research, and the European Interdisciplinary Cybersecurity Conference.