IADIS International Journal on WWW/Internet
Vol. 20, No. 2, pp. 18-34
ISSN: 1645-7641

RAISING INFORMATION SECURITY AWARENESS USING DIGITAL SERIOUS GAMES WITH EMOTIONAL DESIGN

Frauke Prott and Margit Scholl
Technical University of Applied Sciences Wildau, Hochschulring 1, 15745 Wildau, Germany

ABSTRACT

Research studies repeatedly show that, worldwide, violations of security guidelines and data protection regulations often result from unconscious behavior and/or active (flawed) decisions made by individuals. The training and education of users to promote awareness of information security (InfoSec) and appropriate behavior should be one critical and very important component of an organization's security strategy. How can digital serious games make a lasting contribution to raising awareness of InfoSec? In this paper, we present the development and story concept of digital serious games that are guided by emotional design principles such as personalization and storytelling and by the immersive learning approach. The results of user tests reveal that the developed digital serious games are positively accepted by a wide range of employees, moderately support their daily work, and are able to enhance and intensify InfoSec-related knowledge. In particular, women and people under the age of 35 perceive the most benefit from these digital serious games.

KEYWORDS

Emotional Design, Immersive Learning, Digital Serious Games, Awareness, Information Security

1. INTRODUCTION

Successful digitization relies on a high level of information security (InfoSec) (BMI, 2021). The latest Data Breach Investigations Report (DBIR) of Verizon states that 82 percent of the breaches were made possible by unconscious behavior and/or active decisions by humans involving the theft of credentials, phishing, misuse, or error (Verizon, 2022). Thus, the training and education of users to promote awareness of InfoSec and the appropriate behavior required to protect the information and data of their organization should be a critical and very important component of an organization's InfoSec strategy, besides technical advances and the designing

of security guidelines that do not hinder but rather support the carrying out of daily work (Azeroual and Nikiforova, 2022; Sasse et al., 2022; ENISA, 2018).

Accordingly, the focus of this paper is on measures to raise awareness of InfoSec. InfoSec awareness (ISA) in the organizational context is defined as "the extent to which staff understand the importance of information security, the level of security required by the organization and their individual security responsibilities (ISF, 2011, p. 56). A literature review of ENISA (2018) suggests that measures that empower people to respond appropriately to InfoSec threats in the belief that their actions will be successful are more effective in provoking security-conscious behavior than measures that emphasize threats and trigger a feeling of fear. Thus, it is important to arouse positive emotions in employees when raising their awareness. This can be done by integrating emotional design into awareness-raising measures. "Emotional design is the concept of how to create designs that evoke emotions which result in positive user experiences" (Interaction Design Foundation, n.d.). In recent years, serious games have emerged as a new educational approach in InfoSec that creates a fun, enjoyable environment in which users can experience attacks and practice appropriate behavior to protect information assets (Hart et al., 2020).

Against this background, the present paper delineates the development and evaluation of digital serious games using the principles of emotional design to raise awareness of InfoSec for employees working in small and medium-sized enterprises (SMEs). The digital serious games are part of the extensive research project "Awareness Lab SME (ALARM) Information Security", which sets out to innovate a complete scenario that can be used to support SMEs in raising their InfoSec level and fostering a sustainable InfoSec culture within their organizations (https://alarm.wildau.biz/en). This scenario comprises analog and digital learning scenarios (serious games), on-site attacks (such as phishing simulations), and scientific testing, including awareness measurements, quizzes, and tests. The idea is to make InfoSec tangible and to forge an emotional relationship with it at the experiential level. The focus of the results presented here is on the digital serious games.

The paper continues as follows: in section two we give an overview of the research background guiding the development of the digital serious games to raise InfoSec awareness. In section three, we introduce the conceptual background and the story concept of the digital serious games. In section four, we present the results of the user tests of three digital serious games. At the end, in section five we discuss the contribution and limitations of the paper and highlight avenues for future research.

2. RESEARCH BACKGROUND

2.1 Emotional Design of Learning Materials

Emotional design is characterized by, amongst other things, the *personalization* of the user experience, the possibility of *identification*, *appealing multimedia elements* (e.g., visual design, layout, color, sound), and *storytelling* (Interaction Design Foundation, n.d.; Um et al., 2011).

Um et al. (2011) demonstrate that the positive emotional design of multimedia learning materials, comprising saturated, bright warm color combinations and illustrations and characters with round shapes, increases comprehension and transfer and reduces the perceived difficulty

of the learning task. In turn, the positive emotions that are elicited increase motivation and satisfaction and enhance perceptions of the learning materials.

These findings are confirmed in different ways by further studies (e.g., Mayer and Estrella, 2014; Heidig et al., 2015; Li et al., 2020). Using emotional design principles in the design of a PowerPoint lesson—such as designing key learning elements with humanoid features and appealing colors—improves learning outcomes in terms of retention, as compared with standard black-and-white graphics, whereby marginally lower levels of perceived difficulty and marginally higher levels of learning effort are observed (Mayer and Estrella, 2014). In their attempt to identify relevant emotional design features, Heidig et al. (2015) find that learners' emotional states are influenced not so much by the objective but rather by the perceived aesthetics and usability of the material. While a person's emotional state has only a minor effect on learning outcomes, it impacts their intrinsic motivation to learn and to continue working with the learning material (Heidig et al., 2015). By contrast, in a comparison of the test and control groups, Li et al. (2020) do not find there to be any differences in students' emotions when confronted with learning materials with either a positive or neutral design. However, the learning performance differs in that students in the test group performed better in the retention and transfer tests (Li et al., 2020).

When emotional design principles are applied in learning contexts, it is important to make the essential learning content more appealing rather than just adding pretty graphical elements that are irrelevant to the learning content. This practice can impede learning instead of supporting it (Mayer and Estrella, 2014). In general, four conditions should be met for a good learning process (Gabler Wirtschaftslexikon, n.d.): information must appear meaningful, relevant, helpful in people's own work situations, and linked to their existing knowledge. For participants to become actively involved, it is crucial that the topic and the problems of the game are interesting for them (Schell, 2019). Such an interest should be encouraged by an emotional design.

2.2 Game-Based Learning

Emotional design can also be integrated into the learning materials through the use of games and game elements. "The ability to play is critical not only to being happy, but also to sustaining social relationships and being a creative, innovative person" (Brown and Vaughan, 2009, p. 6). Playing is described as being ostensibly purposeless and voluntary, having an inherent attraction, a sense of freedom from time, a diminished consciousness of self, and improvisational potential, and prompting the desire to continue (Brown and Vaughan, 2009). It is suggested that playing affects brain development—for example, by creating new neural connections and benefiting learning (Brown and Vaughan, 2009). "While playing, the brain is able to experience situations without threatening its physical or emotional integrity" (Pavlidis and Markantonatou, 2018, p. 322).

Given the positive effects of play, games and game elements are increasingly being introduced into learning and working environments. Game-based learning (GBL) is described as an enjoyable and motivating form of learning (Linek and Albert, 2009). Serious games are (computer) games used to raise awareness of a topic and to develop knowledge and skills by allowing learners to delve into situations that are seldom or hardly ever experienced (Ypsilanti et al., 2014). In contrast to entertaining games, serious games aim to convey educational content in addition to providing entertainment (Mildner and Mueller, 2016).

Games that are supposed to support learning are characterized by clear objectives and direct feedback (Fang et al., 2013). The participants work toward a specific goal, choose and perform actions, and experience the immediate consequences. GBL and serious games provide learners with an environment in which they can make mistakes and experiment in a protected space (Trybus, 2014).

Studies reveal the positive effects of using games in learning: GBL environments are highly involving and therefore effectively support the learning process (Buffum et al., 2015). Games as a learning method improve short- and long-term learning results (Wouters et al., 2013). Game-based learning scenarios increase motivation and stimulate behavioral change (Bösche and Kattner, 2011; Hsu et al., 2008). It is important to align the games to the everyday reality of the target group, as the connection to real situations and challenges enhances learning success (Lombardi, 2007). Serious games promote learning success through the active involvement of the learners who are able, as a result, to refer to real situations (Ypsilanti et al., 2014).

Meaningful narratives support the immersion in serious games, which is crucial for learning success (Naul and Liu, 2020). Stories support teaching as they a) are more suited to raising interest in a topic compared to, for example, PowerPoint slides conveying information and hard facts, b) give the learning material a context so that the individual learning elements are easier to recall—for example, by creating vivid images—and c) help motivate learners to engage with abstract, possibly challenging learning content, inasmuch as they provide a non-threatening way into a topic (Green, 2004). Thus, stories make the learning content personally relevant and thereby support the learning process (Landrum et al., 2019). Because of these benefits, research documents the effectiveness of storytelling for teaching and learning. The main benefit of storytelling is that its narrative structure and the emotional involvement of learners promote retention of the learning content (Landrum et al., 2019). Thus, good narratives of serious games invite the player to participate in the story and decide on the development of the story, thus encouraging the intrinsic motivation to learn. It is recommended that the narratives stimulate the imagination and include characters with whom learners can empathize (Naul and Liu, 2020).

2.3 Raising InfoSec Awareness

A literature review revealed that self-efficacy is a moderately strong predictor of security-conscious behavior (ENISA, 2018). The concept of self-efficacy describes a person's subjective perception of their own ability to complete a task or achieve a goal. If a person is confident of their own skills, it is more likely that they will successfully complete tasks and achieve goals (Bandura, 1995). Self-efficacy is enhanced by positive personal experiences, a positive perception of other people's experience, and positive feedback and encouragement (Bandura, 1995). Hence, awareness-raising measures should strengthen the perception of self-efficacy in relation to security-conscious behavior. However, ISA often only involves the transfer of knowledge—e.g., via a web-based training or a lecture (Hart et al., 2020; ACS, 2016; Beyer et al., 2015). Yet the complexity of an issue like InfoSec and the relevance of self-efficacy underline the importance of actively involving users in awareness-raising measures so that they are able to protect sensitive information in case of an InfoSec threat or attack. Thus, employees should be given the possibility of experiencing InfoSec threats in a protected space, where they can try out and practice security-conscious behavior. Game-based learning in the form of serious games is a didactic method that enables exactly that (Ghazvini and Shukur, 2018).

Thus, in recent years an increasing number of both research projects and commercial providers have been developing serious games to complement knowledge-based security trainings. Hart et al. (2020) provide an overview of the most established security-related serious games, majoritarian analog (card and board) games. They identify the limitations of the security games they review, stating that the games often focus on a particular category of threats, are developed for a specific context, and do not offer the possibility of considering the security threats from the perspective both of the attacker and of the defender. By contrast, a previous overview and evaluation of serious games in cybersecurity training only focused on digital games in academic and commercial settings (Hendrix et al., 2016). From the perspective of Hendrix et al. (2016), the digital games under review seldom target IT professionals and managers, and the evaluations of them are not sufficiently rigorous.

Research projects report the positive effects of both analog and digital serious security games on participants' engagement and participation in the learning scenarios as well as on learning outcomes (for example, Hart et al, 2020; Yasin et al., 2019; Ghazvini and Shukur, 2018). Moreover, commercial providers of security serious games highlight the positive effects of these awareness-raising and training measures for InfoSec but, as Hendrix et al. (2016) point out, provide no evidence proving these positive outcomes (for example, Kaspersky, 2022; Fabula Games, 2022).

3. DEVELOPMENT OF THE PRESENT DIGITAL SERIOUS GAMES

3.1 Conceptual Background

The development of the digital serious games is guided by the emotional design principles (personalization, identification, appealing multimedia elements, and storytelling (see 2.1)), the research findings—especially relating to the existing limitations of security games—and the intention to enable immersive learning. Immersive learning is a learner-centered approach that should encompass the elements immersion, engagement, risk/creativity, and agency (Blashki et al., 2007). According to Blashki et al. (2007, p. 411) immersion means "the active involvement of physical, emotional and cognitive processes and concentration." Engagement refers to "the user's prolonged interest." Risk/creativity, in turn, is understood as the possibility of taking risks and leaving one's comfort zone, albeit in a protected learning environment, to overcome habits. Agency means that the user has control over her/his learning and playing process (Blashki et al., 2007).

Even if the developer of a serious game cannot accommodate all the qualities of play (Brown and Vaughan, 2009)—e.g., apparent purposelessness—we hope to benefit from these characteristic features in raising awareness of InfoSec and in transferring the relevant knowledge. Thus, we expect that the inherent attraction of play will motivate participants to *engage* with the serious games. The temporal freedom experienced while playing—which we interpret as forgetting time—may encourage users to *immerse* themselves deeper in the topic and learning content than they would with more classical learning materials such as presentations or web-based trainings. The diminished consciousness of self may support *identification* with the game characters, allowing learners to slip into these roles in the serious games and thus experience problems and situations from their perspectives. We also hope to benefit from participants' desire to continue, whereby people who have tried one digital serious game will want to play further serious games dealing with InfoSec issues.

3.2 Story Concept

The digital serious games we are developing consist of *stories* that represent daily work situations in SMEs. The participants experience the stories from a first-person perspective. This supports *immersion*—i.e., the intensive involvement of the users—and enables their *identification* with the learning content. It is expected that it will make the development of knowledge and skills particularly effective and long-lasting. It also enables positive personal experiences and positive feedback as a means to enhance self-efficacy.

As a format, we have chosen the visual novel—a kind of interactive book, in which the players make decisions and thus determine the further course of the story (Choi, 2019). Hence, the digital serious games are characterized by the following *appealing multimedia elements*: pictures in the form of colorful drawings, written dialogues in boxes with rounded corners, and descriptions of the situation. Three-dimensionality is created with the help of ambient music and sound effects (e.g., a person clearing their throat, the phone ringing, a door slamming). Together with the first-person perspective the visual novel format provides *agency* to the users as they make their own decisions, take the consequences, and experience their impact.

The story concept of the seven digital serious games is characterized by diversity, individuality, and continuity. Each game focuses on a different InfoSec issue, such as passwords, CEO Fraud, cloud applications, and data protection. In this way, we intend to address a plurality of possible InfoSec threats. To actively engage participants, it is critical that the topics and problems addressed by the games are relevant and interesting for them (Schell, 2019). Thus, the topics covered in the seven digital games emerged from a qualitative study, one of whose aims was to reveal relevant InfoSec issues in SMEs (Pokoyski et al., 2021). Within these games, the players take on a variety of roles—they may switch from being a security expert to being a hacker, while at another time they may be a detective or even slip inside an artificial intelligence (AI) entity. This not only ensures variety but also enables learners to gain insight into the topics from different perspectives, thus overcoming the limitations of existing security games, as ascertained by Hart et al. (2020). All these measures should elicit *engagement* on the part of the users. Furthermore, the different topics the users experience within the games and the diverse roles they slip into allow them to also experience, in a protected space, *risky* situations that may be unusual for them.

The seven digital games can be played independently of one another and in any order. The individual stories and learning content are self-contained. The specific topics can thus be explored in greater depth and breadth than is possible in a more comprehensive game that includes all the different aspects. Nevertheless, the stories are interconnected by an overall storyline that plays out in a fictional organization. As a result, the participants meet the same people (boss, departmental manager, trainee, production manager) in each serious game and get to know them better.

Each digital serious game offers a *personalized* learning experience. At the beginning, the participants choose a character and a name. With every decision that has an impact on the course of the game, the players embark on their very own learning journey based on their knowledge and preferences. Each game includes two to three learning paths that the users follow based on their decisions. The paths that are chosen determine the learning content that the participants are confronted with and the challenges they have to meet. In each game the users can enhance different skills (e.g., social competence) and areas of knowledge (e.g., security understanding) that are important for InfoSec.

One character in the overall story welcomes the participants at the beginning of a digital game and alerts them to the topic of the game, to the skills and knowledge that are evaluated within the game, and to aspects the users should concentrate on. At the end of the game, the same character gives feedback on what has been achieved. This feedback includes an explanation of how the score was calculated and recommendations and suggestions for the user. Other feedback messages are shown during the game and indicate positive and negative decisions and behavior. In addition, a glossary module allows learners to read important InfoSec terms before and after the digital game. Hence, the users are not left to their own devices but are supported while learning. Figure 1 shows screenshots of a decision option within the digital game and of feedback at the end of it.

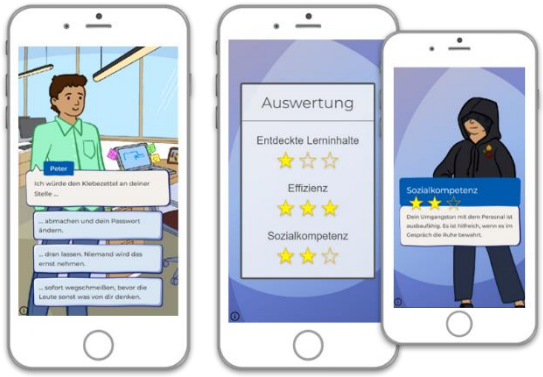

Figure 1. Sample screenshots of alternative decisions and feedback at the end of a game

4. USER TEST OF THREE DIGITAL SERIOUS GAMES

4.1 Test Users

The digital serious games developed in the present project are particularly tailored to the employees and management of SMEs who work in different departments—performing different sets of tasks—and are not experts in information technology. Employees from the pilot companies and other partner organizations test and evaluate the digital serious games from a practical perspective. The contact persons at these organizations receive the information about the user test and forward it to employees. Staff participation is voluntary so that the most important aspect of rules agency, "to decide to play, or not to play" (Duarte and Holanda, 2022), is met. Thus, we have no influence over which employees ultimately take part. The responses by the test users form the basis for the final development of these serious games.

The user test includes short, standardized, written pre- and post-surveys that are analyzed descriptively. The participants are asked about the extent to which they agree with given statements on a five-point Likert scale—focusing, for example, on content, the realism of the presentations, the playing time, and the level of difficulty. Learning success is measured by self-assessments reflecting on the acquisition and deepening of knowledge.

In the following, we present the results of the user tests of three digital serious games. In the first, called *Hacker Attack*, the users slip into the role of a hacker who tries to log in to the server of the fictional company. The scores in this game relate to efficacy (Do the users succeed in the hack?) and variability (How many different approaches have the users tried in attempting to achieve their goal?). In the second, *Search for Clues*, the users take on the role of a detective who is trying to solve a case of CEO Fraud in the fictional company. Here, the users are assessed in terms of their efficacy (Do they manage to solve the case?), social competence (Do they treat the employees of the company in an empathic and friendly manner?), and discovered learning content (How much learning content do they encounter on their way through the game?). In the third game, *AI in the Home Office*, the users—in the role of an AI entity—search for the most common weaknesses while working in the home office. In this game, the focus of the assessment is on a sound security awareness and the success of the users in predicting human behavior.

Table 1. Sample composition[1]

Sample characteristic	**Hacker Attack (n=26)**	**Search for Clues (n=23)**	**AI in the Home Office (n=15)**
Sex	31% female 65% male 4% unspecified	57% female 35% male 4% diverse 4% unspecified	44% female 33% male 19% unspecified
Age	15% 14–24 35% 25–34 35% 35–50 15% 50+	9% 14–24 22% 25–34 43% 35–50 26% 50+	31% 25–34 31% 35–50 27% 50+ 6% unspecified
Department	23% sales 19% human resources 15% IT 12% customer service 8% (each) procurement, research and development 4% (each) production, public relations, administration office, management	30% human resources 17% customer service 17% sales 9% (each) research and development, IT, public relations 4% (each) legal department, management	25% research and development 19% human resources 13% IT 6% (each) customer service, marketing, public relations, administrative office, sales, management, unspecified

Table 1 provides information about the sample composition of the three user tests. The participants of the first user test of the game *Hacker Attack* were mostly male (65%, n=26[2]) with two predominant age ranges: 25–34 (35%) and 35–50 (35%). They mostly worked in the fields of sales (23%), human resources (19%), and information technology (IT) (15%). By contrast, the participants in the second user test of the digital game *Search for Clues* were predominantly female (57%, n=23) and most of them were between 35 and 50 years old (43%). They were primarily employees in the human resources (30%), customer service (17%), and sales (17%) departments. The test users of *AI in the Home Office* are more evenly distributed in regard to

[1] Values of 99% or 101% are due to rounding.

[2] The differing sample size (n) is determined by the fact that not all participants took part in both the pre- and post-questionnaire or answered all the questions.

sex (44% female, 33% male, n=15) and age (31% 25–34, 35–50, respectively, and 27% 50+). The participants of this third user test predominantly work in the fields of research and development (25%), human resources (19%), and IT (13%).

4.2 Overall Evaluation

The participants needed an average of ten to twelve minutes to complete the games (*Hacker Attack*: 10 minutes, n=42; *Search for Clues*: 10 minutes, n=31; *AI in the Home Office:* 12 minutes n=19). The users evaluated the playing time on average as "exactly right" on a five-point Likert scale (1=too short, 3=exactly right, 5=too long) (*Hacker Attack*: mean=3, n=31; *Search for Clues*: mean=3.44, n=25; *AI in the Home Office*: mean: 3.47, n=15). The perceived level of difficulty is between "easy" and "exactly right" with a mean of 2.81 for *Hacker Attack* (n=31), 2.52 for *Search for Clues* (n=25), and 2.80 for *AI in the Home Office* (n=15) (scale: 1=too easy, 3=exactly right, 5=too difficult).

Figure 2 (below) shows the overall assessment of the three digital serious games from the perspective of the test users. We interpret the midpoint of the scale (=3) to mean "good" in the user evaluation, expressing satisfaction on the part of respondents. We do so because of the different demographics of the test users (see Table 1) and the assumption of different preferences for playing in general and for video games in particular. In addition, studies indicate that the left end of a response scale is selected more often than the right (Menold and Bogner, 2015). Thus, in our opinion the three serious games receive a relatively positive evaluation, as almost all the aspects score an average value of over 3.

We were interested to know if the developed digital serious games appeal to different people depending on their sex and age. We therefore analyzed the responses separately by sex (i.e., female, male) and age group (i.e., 14–24, 25–34, 35–50, 50+). Women evaluated all three digital serious games better than men. Whereas the difference between female and male users across all statements of the overall evaluation is about 0.43 for *Hacker Attack* and 0.33 for *Search for Clues*, the difference found between the two sexes in the overall evaluation of *AI in the Home Office* comprises 0.98.

We also discovered differences between the age groups. Figures 3–5 illustrate that younger test users (aged 14–34) tend to evaluate the digital serious games more positively than older age groups (aged 35+), with the exception of test users over the age of 50 in the case of *AI in the Home Office*.

The overall positive evaluation of the digital serious games and the relatively high level of agreement with the statement that users would like to play further serious games of this kind (see Figure 2) show that, bearing in mind the different demographics of those taking part in the user tests (see Table 1), a wide range of users enjoy these kinds of games as awareness-raising measures. However, as users are less motivated to play the same digital serious game again (mean value between 2.20 and 2.48 for the three games, see Figure 2), it is important to integrate the digital serious games in a broader awareness-raising measure that includes other materials to reinforce the process.

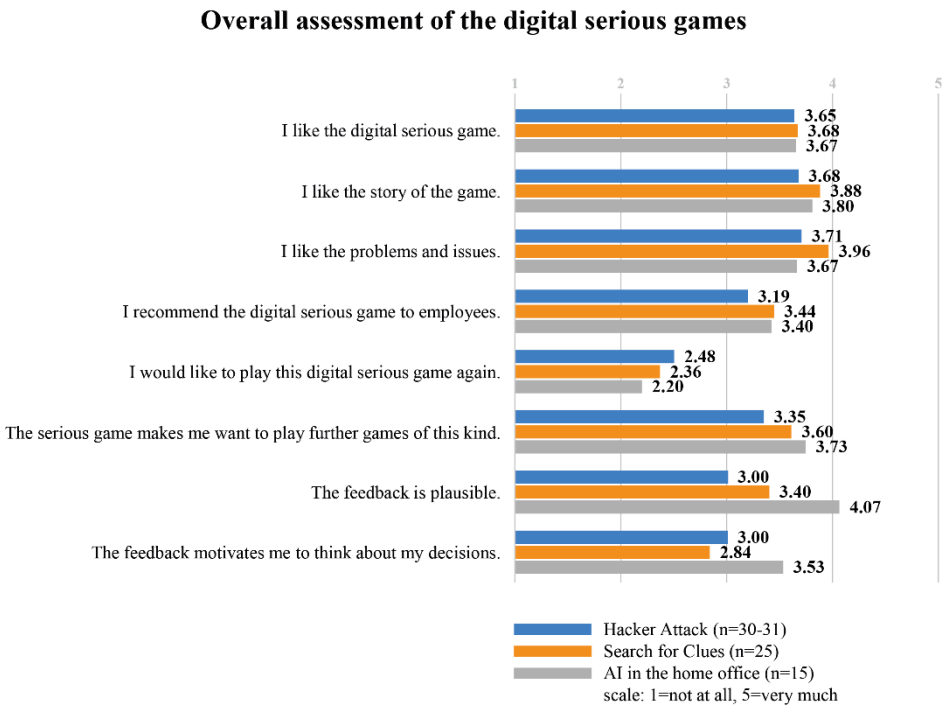

Figure 2. Overall assessment of the digital serious games *Hacker Attack*, *Search for Clues*, and *AI in the Home Office*

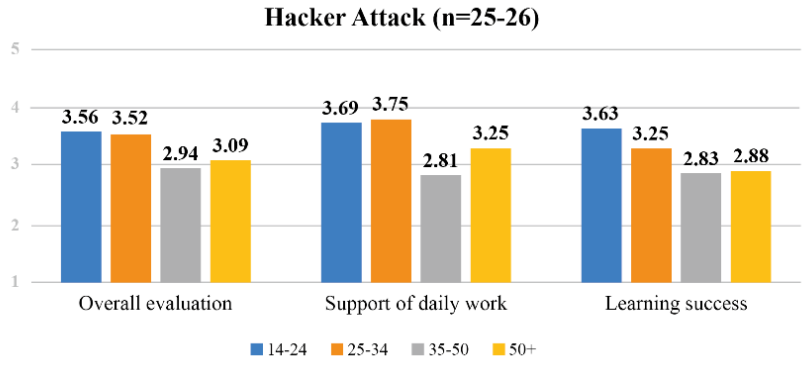

Figure 3. Overall evaluation, assessment of support of daily work and learning success of the digital serious game *Hacker Attack* by different age groups

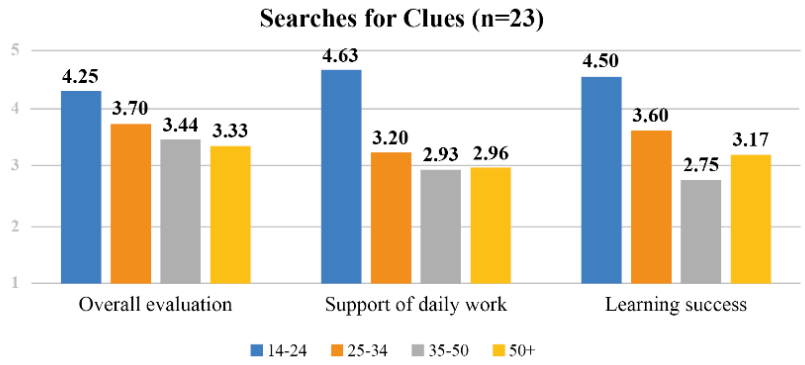

Figure 4. Overall evaluation, assessment of support of daily work and learning success of the digital serious game *Search for Clues* by different age groups

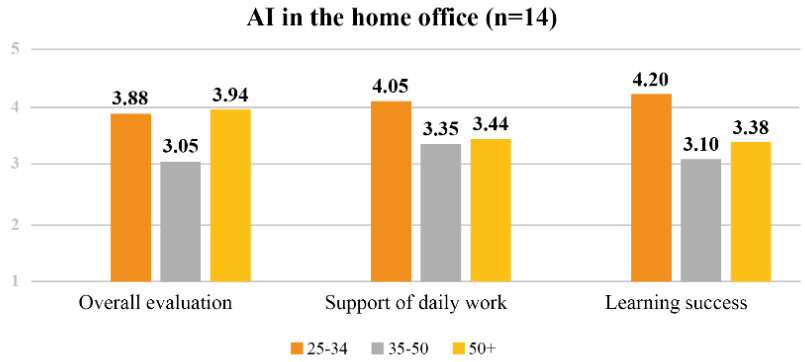

Figure 5. Overall evaluation, assessment of support of daily work and learning success of the digital serious game *AI in the Home Office* by different age groups[3]

4.3 Support of Daily Work

Figure 6 shows that the narratives of the digital serious games moderately reflect the working lives of users and that they—and therefore the learning content provided—moderately support them in their daily working life. It is striking that the game *AI in the Home Office* performs best on these questions. In our opinion, this reflects the fact that probably all test users have experience of working at home. Conversely, they may not have any experience relating to the other two digital serious games—hacker attack and CEO fraud. Thus, the test users perceive the third digital serious game as being most beneficial for their daily work. This finding and the fact that the third digital serious game also ranks highest for the statement "The serious game makes me want to play further games of this kind" (see Figure 2) underline that *engagement* in learning is best achieved if the topics of the games are relevant to users.

[3] In the case of *AI in the Home Office*, no test user was part of the group aged 14–24.

To raise awareness of the relevance of all the topics dealt with in the individual digital serious games, and in response to comments from the post-survey, we will integrate the lessons learned in each digital serious game at the end of the feedback process. This is in line with the findings of Lacruz and Américo (2018) that the quantum of learning is on average 18 percent higher if participants are involved in a debriefing after a business game.

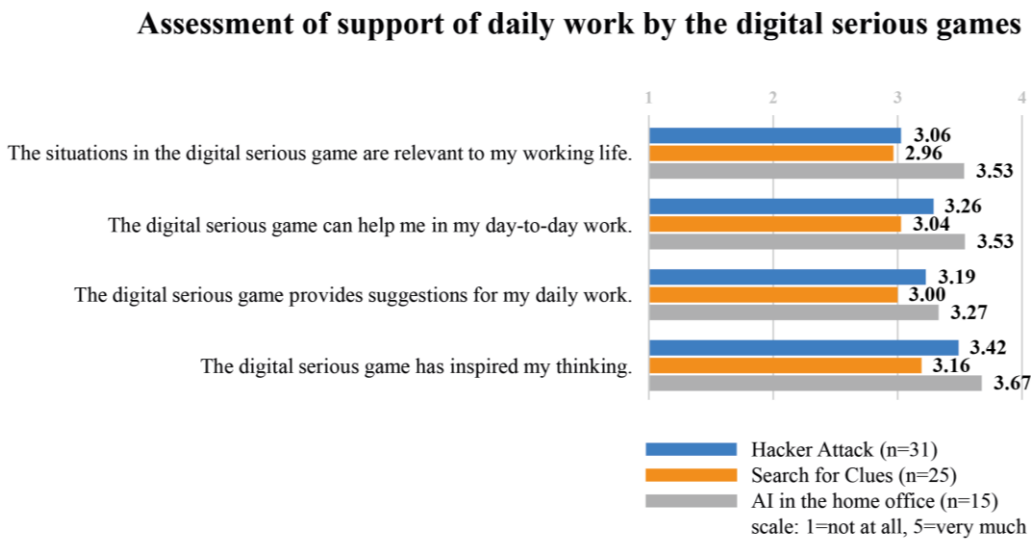

Figure 6. Assessment of the degree to which daily work is supported by the digital serious games *Hacker Attack*, *Search for Clues*, and *AI in the Home Office*

In analyzing the four questions about the effect of the games on the daily work of the three departments most represented in the user tests, it is striking that human resources agreed most strongly with the given statements. For the digital serious games *Hacker Attack* and *Search for Clues*, sales agreed least strongly and for the digital serious game *AI in the Home Office*, IT agreed least strongly with the given statements. These analyses help us to formulate recommendations about which digital serious game is best suited to raising the InfoSec awareness of which employees.

Analogous to the overall evaluation, the female users assessed the relevance and the support of the digital serious games for their daily work higher than the male test users. In the case of *Hacker Attack* and *Search for Clues*, the difference between women and men over these four statements is rather small and comprises 0.24 and 0.32 respectively. Again, the discrepancy in the case of *AI in the Home Office* between female and male test users is relatively high with a value of 1.31.

In line with the overall evaluation, the question relating to the support provided by the digital serious games in people's daily work is given a higher rating by younger than by older test users. The 35–50 age group agreed least strongly, on average, with the four statements (see Figures 3–5).

4.4 Learning Success

The participants have a sense of learning success when playing the digital serious games. They acquired new knowledge or reinforced what they already knew. In Figure 7, the mean values of the agreement with these two statements are illustrated.

Again, we found differences between the sexes and the age groups in answering these questions. Female test users perceived on average a higher learning success compared to men (*Hacker Attack* (n=25): $\Delta_{women\text{-}men}$=0.46; *Search for Clues* (n=21): $\Delta_{women\text{-}men}$=0.42; *AI in the Home Office* (n=12): $\Delta_{women\text{-}men}$=1.37). Test users under the age of 35 perceived a higher degree of learning success as compared with older participants. The 35–50 age group agreed least that they acquired new knowledge and deepened their existing competence (see Figures 3–5).

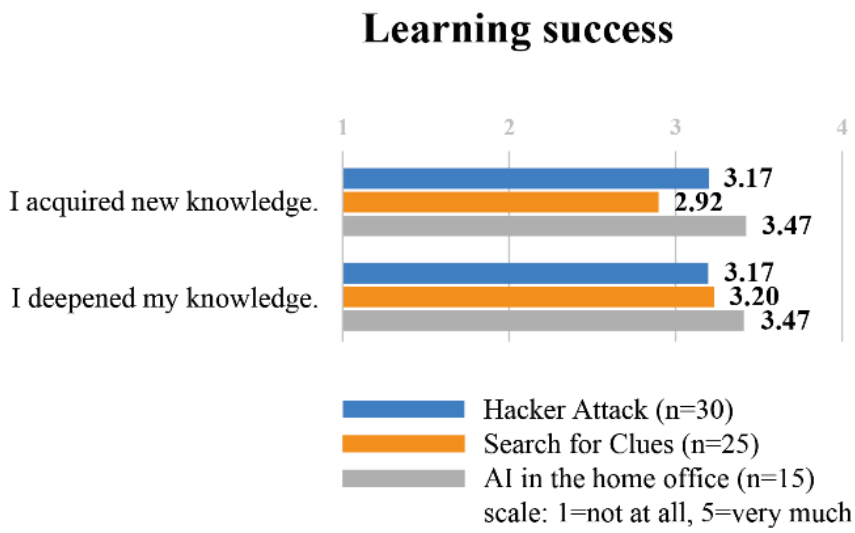

Figure 7. Perceived learning success as a result of playing the digital serious games *Hacker Attack*, *Search for Clues*, and *AI in the Home Office*

5. DISCUSSION

5.1 Research and Practical Contribution

The results of the user tests indicate that digital serious games that use emotional design principles, such as personalization, the possibility for identification, appealing multimedia elements, and storytelling, are positively accepted by employees and moderately help to enhance and intensify knowledge in the area of InfoSec. The digital serious games also support users to some degree in their daily work. These games are thus a promising measure for raising awareness of InfoSec.

The three digital serious games that are presented here have been developed as part of a research project designed for employees in SMEs—raising awareness of InfoSec topics is relevant for their professional life in general and, to a certain extent, for their private life (passwords, phone fraud, etc.). The serious games and the underlying research project have added social value, as the games and other materials developed in the project are available on the dedicated website free of charge for anyone interested.

Thus, for example, organizations can raise employee awareness of InfoSec while expending fewer resources. The digital serious games can also become part of the education of young adults, enabling apprentices and students to start their professional life with an awareness of InfoSec.

5.2 Limitations and Further Research

InfoSec is an issue that is constantly evolving. Thus, it is important that the serious games cover different topics—as is the case here—and are, if possible, updated from time to time. In addition, the digital games should be part of a wider awareness-raising measure, as in the present research project. We intend to include further recommendations for users at the end of a digital serious game. Based on their results in the specific digital game, the users should be referred to other digital serious games, which they can use to practice the same or other InfoSec skills and knowledge. They will also be invited to participate in a test where they can broaden their knowledge of the subject that the digital game focuses on.

It is not possible to reliably conclude, on the basis of the self-assessments of the test users, that the digital serious games enhance and intensify knowledge while also raising awareness and ultimately encouraging safe behavior. A more elaborated scientific methodological approach to measuring InfoSec awareness and behavior (intention) is warranted to validate the first preliminary findings of these user tests. We are therefore using the current research project to develop and test an instrument for measuring InfoSec awareness including security-conscious behavior.

An important component of social constructivist principles, which immersive learning builds on (Blashki et al., 2007), is that knowledge is constructed, acquired, and enhanced in the exchange with other learners (Reich, 2006). In line with this, we observed that the discursive exchange of experience and knowledge during and after a session playing *analog* serious games, which are also being developed in the project, is critical to raising awareness of InfoSec. Even though the users of the *digital* serious games are supported during the learning process by the feedback and the glossary, further research is needed into ways of stimulating an exchange of ideas between the participants of the digital learning scenarios.

ACKNOWLEDGEMENT

We thank the Federal Ministry for Economic Affairs and Climate Action for funding the project. We are grateful to Gamebook Studio HQ for developing the digital serious games and the pilot companies for their active involvement in the project. Finally, we would like to express our gratitude for the opportunity to expand our conference paper for publication in this journal. Many thanks, too, to Simon Cowper for his detailed and professional proofreading of the text.

REFERENCES

Allianz für Cyber-Sicherheit (ACS) (alliance for cyber security), 2016. *Awareness-Umfrage 2015: Ergebnisse (Awarenss Survey 2015: Results)*. Bonn, Germany.

Azeroual, O. and Nikiforova, A., 2022. Apache Spark and MLlib-Based Intrusion Detection System or How the Big Data Technologies Can Secure the Date. *Information*, Vol. 13, No. 2, article 58.

Bandura, A., 1995. Exercise of Personal and Collective Efficacy in Changing Societies. *In Bandura, A. (ed). Self-efficacy in Changing Societies*. Cambridge University Press, Cambridge, England, pp. 1-45.

Beyer, M., S. et al., 2015. *Awareness is Only the First Step: A Framework for Progressive Engagement of Staff in Cyber Security*. Hewlett Packard, Business white paper.

Blashki, K. et al., 2007. 'The future is old': immersive learning with generation Y engineering students. *European Journal of Engineering Education*, Vol. 32, No. 4, pp. 409-420.

Bösche, W. and Kattner, F., 2011. Fear of (Serious) Digital Games and Game-based Learning? Causes, Consequences and a Possible Countermeasure. *International Journal of Game-Based Learning*, Vol. 1, No. 3, pp. 1-15.

Brown, S. and Vaughan, C., 2009. *Play. How It Shapes the Brain, Opens the Imagination, and Invigorates the Soul.* Avery, Penguin Group, New York, USA.

Buffum, P. S. et al., 2015. Mind the Gap: Improving Gender Equity in Game-Based Learning Environments with Learning Companions. *AIED: International Conferences on Artificial Intelligence in Education*.

Bundesministerium des Innern, für Bau und Heimat (BMI) (Federal Ministry of the Interior and Community), 2021. *Cybersicherheitsstrategie für Deutschland 2021 (Cyber Security Strategy for Germany 2021)*. Berlin, Germany.

Choi, C., 2019. *Bigger on the Inside: A History of Visual Novels.* https://medium.com/@cecilchoi/bigger-on-the-inside-a-history-of-visual-novels-981e42f43608, 22. Februar 2019, accessed May 6, 2022.

Duarte, L. C. S. and Holanda, A., 2022. We Need to Focus on Rules. *Proceedings of the International Conferences on Interfaces and Human Computer Interaction 2022 and Game and Entertainment Technologies 2022*, July 20-22, 2022, pp. 233-236.

European Union Agency for Network and Information Security (ENISA), 2018. *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*. Heraklion, Greece.

Fabula Games, 2022. *Serious Games: Incredibly Effective.* https://fabula-games.de/en/, accessed June 28, 2022.

Fang, X. et al., 2013. Development of an Instrument for Studying Flow in Computer Game Play. *International Journal of Human-Computer Interaction*, Vol. 29, No. 7, pp. 456-470.

Ghazvini, A. and 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 Application*, Vol. 9, No. 9, pp. 236-245.

Gabler Wirtschaftslexikon, n.d.: *Lernen (Learning)*. https://wirtschaftslexikon.gabler.de/definition/lernen-41169, accessed February 04, 2022.

Green, M. C., 2004. Storytelling in Teaching. *aps – Association for Psychological Science*, https://www.psychologicalscience.org/observer/storytelling-in-teaching, accessed September 1, 2022.

Hart, S. et al., 2020. Riskio: A Serious Game for Cyber Security Awareness and Education. *Computer & Security*, Vol. 95, August 2020, article 101827.

Heidig, S. et al., 2015. Emotional Design in Multimedia Learning: Differentiation on Relevant Design Features and Their Effects on Emotions and Learning. *Computers in Human Behavior*, Vol. 44, March 2015, pp. 81-95.

Hendrix, M. et al., 2016. Game Based Cyber Security Training: Are Serious Games suitable for cyber security training? *International Journal of Serious Games,* Vol. 3, No. 1, pp. 53-61.

Hsu, S. H. et al., 2008. From Traditional to Digital: Factors to Integrate Traditional Game-based Learning into Digital Game-based Learning Environment. *Proceedings 2nd IEEE International Conference on Digital Game and Intelligent Toy Enhanced Learning, DIGITEL*, pp. 83-89.

Interaction Design Foundation, n.d.. *Emotional Design.* https://www.interaction-design.org/literature/topics/emotional-design, accessed May 8, 2022.

ISF, 2011. *The 2011 Standard of Good Practice for Information Security.* June 2011. Information Security Forum, https://www.uninett.no/sites/default/files/webfm/ISF%20Standard%20of%20Good%20Practice%20for%20Information%20Security%202011.pdf, accessed September 9, 2022.

Kaspersky, 2022. *[Dis]connected. A mobile cybersecurity quest.* https://media.kaspersky.com/en/business-security/enterprise/Kaspersky_[dis]connected_datasheet_0121EN_Gl.pdf, accessed June 28, 2022.

Lacruz, A. J. and Américo, B. L., 2018. Debriefing's Influence on Learning in Business Game: An Experimental Design. *BBR. Brazilian Business Review*, Vol. 15, No. 2, pp. 192-208.

Landrum, R. E. et al., 2019. The pedagogical power of storytelling. *Scholarship of Teaching and Learning in Psychology*, Vol. 5, No. 3, pp. 247-253.

Li, J., et al., 2020. Can Emotional Design Really Evoke Emotion in Multimedia Learning?. *International Journal of Educational Technology in Higher Education*, Vol. 17, article 24.

Linek, S. B. and Albert, D., 2009. Game-based Learning: Gender-Specific Aspects of Parasocial Interaction and Identification. *International Technology, Education and Development Conference (INTED)*.

Lombardi, M., 2007. *Authentic Learning for the 21st Century: An Overview*. http://www.lmi.ub.edu/cursos/s21/REPOSITORIO/documents/Lombardi_2007_Authentic_learning.pdf, accessed May 12, 2022.

Mayer, R. E. and Estrella, G., 2014. Benefits of Emotional Design in Multimedia Instruction. *Learning and Instruction*, Vol. 33, October 2014, pp. 12-18.

Menold, N. and Bogner, K., 2015. *Gestaltung von Ratingskalen in Fragebögen (Layout of rating scales in questionnaires).* GESIS – Leibniz-Institut für Sozialwissenschaften (SDM Survey Guidelines), Mannheim, Germany.

Mildner, P. and Mueller, F., 2016. Design of Serious Games. *In Dörner, R. et al. (eds). Serious Games: Foundations, Concepts and Practice*. Springer International Publishing, Cham, Switzerland, pp. 57-82.

Naul, E. and Liu, M., 2020. Why Story Matters: A Review of Narrative in Serious Games. *Journal of Educational Computing Research*, Vol. 58, No. 3, pp. 687-707.

Pavlidis, G. P. and Markantonatou, S., 2018. Playful Education and Innovative Gamified Learning Approaches. *In Koutsopoulos, K. C. et al. (eds). Handbook of Research on Educational Design and Cloud Computing in Modern Classroom Settings*. IGI Global, Hershey, Pennsylvania, USA, pp. 321-341.

Pokoyski, D. et al., 2021. *Qualitative Wirkungsanalyse Security Awareness in KMU: Tiefenpsychologische Grundlagenstudie im Projekt Awareness Labor KMU (ALARM) Informationssicherheit (Qualitative Impact Study Security Awareness in SME: Deepthpsychology Fundamental Study in the Project Awareness Lab SME (ALARM) Information Security).* Scholl, M. (ed), Technische Hochschule Wildau (Technical University of Applied Sciences Wildau), Wildau, Germany. https://alarm.wildau.biz/static/d6490e49f8d31adfa35259134b8d1b9d/220316-alarm-studie-final.pdf, accessed May 6, 2022.

Reich, K., 2006. *Konstruktivistische Didaktik. Lehr- und Studienbuch mit Methodenpool (Constructivist Didactics. Textbook and Studybook with Collection of Methods).* Beltz Verlag, Weinheim, Basel, Germany, Switzerland.

Sasse, A. et al., 2022. Warum IT-Sicherheit in Organisationen einen Neustart braucht (Why IT-Security in Organizations needs a restart). *18. Deutscher IT-Sicherheitskongress des BSI (18. German IT-Security Convention of the BSI (Federal Office for Information Security).*

Schell, J., 2019. *The Art of Game Design. A Book of Lenses*. 3rd edition. CRC Press, London, England.

Trybus, J., 2014. *Game-Based Learning: What it is, Why it Works, and Where it's Going.* New Media Institute.

Um, E. et al., 2012. Emotional Design in Multimedia Learning. *Journal of Educational Psychology*, Vol. 104, No. 2, pp. 485-498.

Verizon, 2022. *Data Breach Investigations Report (DBIR) 2022*. https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf, accessed June 28, 2022.

Wouters, P. et al., 2013. A Meta-analysis of the Cognitive and Motivational Effects of Serious Games. *Journal of Educational Psychology*, Vol. 105, No. 2, pp. 249-265.

Yasin, A. et al., 2019. Improving software security awareness using a serious game. *IET Software*, Vol. 13, No. 2, pp. 159-169.

Ypsilanti, A. et al., 2014. Are Serious Video Games Something More than a Game? A Review on the Effectiveness of Serious Games to Facilitate Intergenerational Learning. *Education and Information Technologies*, Vol. 19, pp. 515-529.