Enhancing Game-Based Learning Through Infographics in the Context of Smart Home Security

Mehrdad Bahrini, Nima Zargham, Johannes Pfau, Stella Lemke, Karsten Sohr, Rainer Malaka

Enhancing Game-Based Learning Through Infographics in the Context of Smart Home Security

Mehrdad Bahrini[1], Nima Zargham[1], Johannes Pfau[1], Stella Lemke[1], Karsten Sohr[1], and Rainer Malaka[1]

Digital Media Lab, TZI, University of Bremen, Bremen, Germany
{mbahrini,zargham,jpfau,slemke,sohr,malaka}@uni-bremen.de

Abstract. Constantly evolving advances of smart home devices features require users to persistently keep up with safety concerns. While update reports and news articles are common ways to keep them informed, many users struggle in thoroughly understanding and applying available security recommendations. Educational games have proven to be an intuitive way to increase the incentive for awareness but many of them come short to convey the needed supporting knowledge. In an attempt to raise security awareness on smart home devices, we designed an educational game to demonstrate the latest security challenges and solutions. To ascertain users' attention and motivation, we have developed two versions of the game to contrast the integration of text and infographics as supporting knowledge which are the hints in this case. Our evaluations give evidence that viewing security-related content with a higher deployment of infographics improves users' performance significantly, increases users' interest in the topic, and creates higher levels of confidence solving security problems and complexities.

Keywords: Usable Security · Smart Home · Educational Games · Supporting Knowledge · Infographics.

1 Introduction

Educational games (edu-games) have shown great potential in being a powerful teaching tool as they can increase engagement, creativity and authentic learning [23, 38, 60]. Game-based learning allows users to see themselves in simulated real situations where they can learn through experience and solve the problems through critical thinking [13]. Furthermore, the motivational power of game-based learning towards specific subjects is widely recognised [31]. Harnessing the intrinsically motivating power of games, researches have shown that edu-games can be a great tool to promote user engagement and improve positive usage patterns, such as increasing user activity, social interaction, and the quality and productivity of user actions [22, 37]. Previous work has shown that edu-games can be useful in raising the knowledge and awareness of the users [3, 60], but this alone can not get the best out of the learning experience.

In edu-games, feedback plays a key role in providing the user the necessary information for the learning experience. Using in-game feedback is intended to guide learners to improve their performance, and increase motivation or learning outcomes by providing them with information on the accuracy of their answers in various ways [62]. According to Johnson et al. [35], these feedback messages can be classified into two types. *Outcome-oriented* feedback delivers information to learners about their progress or the accuracy of their answers (e.g. which is the correct answer and why). *Process-oriented* feedback provides learning guidance and supporting knowledge on the processes as well as strategies used to achieve the correct answer or action in the game. Examples of process-oriented feedback are prompts and hints that lead the learners towards the right answer. In many video games, supporting knowledge is used to inform the players about their objectives and guide them throughout the game. This form of process-oriented feedback could be leveraged to improve the effectiveness of educational games [56]. The supporting knowledge can be given to the users in different forms such as text, images, audio, and video, to provide explicit guidance to players as they play the game [35]. In this paper, we study the use of infographics as a way to convey information to the players in an edu-game.

Infographics are a graphical representation of information or knowledge [33]. They are essentially an effective visual representation that explains information simply and quickly using a combination of text and graphical symbols. Some commercial games such as Metrico+ [24], Mini Metro [16], and Lumino City [57] have implemented infographics as their look-and-feel or even game mechanic and have received very positive reviews from the users. Infographics can motivate players and exploit the visual potential to represent and convey knowledge. They aim to increase the amount of information people remember by breaking them into concise, visually attractive chunks of data. This way, the learners can remember more, leading to improvement in their capabilities [8]. Although utilizing infographics have shown to be effective in transferring information, the implementation of infographics in edu-games is still under investigation.

Recent innovations in technology and the rise of inter-connectivity between devices enable the development of innovative solutions in the field of smart homes to take advantage of these opportunities. Along with this rapid development, the security and privacy of users has always been a concern. Making smart home devices more secure may partly address this concern, but users also have a complementary role in protecting their sensitive information. However, users' understanding and ability to adopt and configure the security of smart home devices is not integrated. As users face a plethora of innovations as well as the ever-expanding spread of security news and journals, it has become increasingly difficult for non-tech-savvy users to understand and apply security guidance. Games have long been recognized as an effective and appealing educational strategy in the field of computer security and privacy [61]. This approach has been used to teach various topics related to security [29, 21].

We have designed an edu-game with the aim of aiding owners of smart home devices to get acquainted with security issues and recent risks. Players are asked

to find potential smart home devices in different rooms and answer questions about the respective device, helping a virtual smart home owner to protect his home from attacks. For contentual assistance during the game, players have the opportunity to assess security instructions concerning the respective device. Within our evaluation, this information is presented textually (analogous to conventional safety reports or updates) or visualized using infographics, as a structured combination of text, images, charts, and icons. Eventually, infographics aim to enable effective representation of data and explain complex problems in a clear and understandable way [30]. Using a between-subjects design, we investigate the users' motivation and evaluate the impact of infographics on players, to answer the following research question: *To what extent can infographics as supporting knowledge improve the learning experience of users and make learning more effective in an educational game in a smart home security context?*

Our results indicated a significant amount of correct answers, as well as an increase of perceived competence by the introduction of infographics. Harnessing this motivation and illustration potential, this paper augments the area of educational serious games with immediately comprehensible knowledge representation and provides evidence that players are more effective, motivated and spend more time on self-education by the implementation of infographics.

2 Related Work

2.1 Game-Based Learning for Security Topics

Game-based learning uses different techniques to manipulate the behavior of users in the direction of a specific goal within a non-gaming context [27]. For example, it can be utilized as a marketing strategy to promote products or services or for training and simulating complex environments virtually [70]. Games can establish the facilitation of enjoyment and engagement by increasing intrinsic motivation, in contexts that are primarily extrinsically motivated. Game-based learning approaches, especially mobile learning [28], are a relatively new approach to security education. A study comparing the use of text, videos, and games found that mobile learning can raise awareness of security issues and teaches users more effectively in comparison to the traditional text-based and video-based learning materials [1].

Research studies showed that serious games provide promising ways to change cybersecurity behaviour [19]. Bahrini et al. [6] developed a gamified application that helps users to understand the consequences of granting permissions to the applications. Their results showed that playing the gamified application results in a significant increase of player enjoyment and that the game is more informative than the traditional approach of permission administration via the Android system settings.

In an attempt to raise interest and awareness towards the topic of privacy and security settings of mobile devices, Zargham et al. developed a humorous decision-making game that helps users to better understand the consequences of

applying security changes on a mobile device [68]. They compared their game to two more models (a serious animated video and a humorous animated video) and found that the game-based approach is more successful in engaging and raising awareness.

Wen et al. designed and developed a role-playing game to engage users to learn more about phishing threats in an active and entertaining manner [67]. Their study showed that the game raises awareness towards the topic and enhances anti-phishing self-efficacy facing phishing emails. Chen et al. presented a desktop game, aiming to change cybersecurity behavior by translating self-efficacy into game design [14]. Their results showed that the game experience could improve users' confidence in tackling security issues.

Many studies have explored the effectiveness of games for increasing cybersecurity awareness, however, most of them have focused primarily on factors of entertainment or engagement of such games, and very little on the learning effect and behavioural change in users [32, 2].

2.2 Supporting Information in Game-Based Learning

Edu-games are seen as one of the most promising forms of computer-based education and multiple studies have shown their highly engaging potentials [54, 34]. Nonetheless, there is less support for their educational effectiveness [20, 66, 43]. Many of the existing work did not evaluate the effectiveness of the components used in an edu-game. One element of the game that is particularly easy to adapt and can have a considerable influence on motivation is feedback. Studies have indicated that in computer-based learning environments, feedback can be a confirmation of a correct answer or an explanation or recommendation in detail. Detailed feedback has a greater impact on learning outcomes and motivation than simple feedback, but this depends on the learners' attention and ability to correct their actions [11, 59].

In an attempt to study the effectiveness of hints, O'Rourke et al. gathered data from 50,000 students and compared four different hint designs based on successful hint systems in intelligent tutoring systems and commercial games [52]. Their results showed that all four hint systems negatively impacted performance compared to a baseline condition with no hints. Authors also suggest that traditional hint systems may not translate well into the educational game environment.

Appropriate presentation of the feedback could have a considerable impact on the effectiveness of the players and can promote deep, meaningful learning [50]. Studies have shown that people learn more deeply when words are presented in spoken form rather than in printed form [55, 25]. However, they did not suggest that feedback should always be presented as spoken words. In this paper we evaluate an approach for comparing text and infographics as *process-oriented* feedback and their impact on the user experience and game outcome.

2.3 Infographics

Information is remembered better when it is supported with pictures [42]. The use of visual information during learning and instructional processes offers many advantages. Studies showed that if a text is followed by illustrations, learners retain information for longer and are more likely to remember it [18, 47, 46, 5, 15, 53]. Infographics are a powerful way to distill and explain complex information as a visual narrative and constitute an effective way of communicating data to decision makers who need high-quality information in a bite-sized and easily accessible form [41]. Visual embellishments, including recognizable comics and images make infographics effective and improve data presentation and memorability [7, 9].

Studies show that infographics brings various modalities together in the hope that they will be understood by a wider audience, regardless of their ability to learn. Infographics use text and illustrations or images to inspire readers to better remember the information presented [45]. Following a study by Kay and Terry [39], they argued that inclusion could be achieved through the use of iconic symbols, short facts and captions as a means of highlighting relevant important information in complex documents. Similarly, Knijnenburg and Cherry [40] suggested using comics as a more inviting, understandable and engaging medium to improve the communication of privacy notices.

Unlike the efforts made to explore the effects of infographics [41, 45], research on the use of infographics in edu-games has not been studied thoroughly. This paper showcases the potential of using infographics embedded in an educational game. We aim to aid users in becoming more familiar with security concepts of their devices and motivate them to increase their knowledge on the topic. Our approach is focused on providing efficient process-oriented feedback in the context of security to help with the understanding of security issues in the smart home environment.

3 Approach

We designed an educational game that uses infographics as supporting knowledge in an approach to raise players' awareness and increase their interest towards smart home security issues. The learners explore the game levels to interact with smart devices and answer a number of security questions (see Figure 1). The provided supporting information helps the players to answer the questions and gain a deeper understanding of the new security concerns of smart devices.

The game was developed for mobile platforms and has an ordinary person narrative. At the beginning of the game, the player meets the character "Luca" in front of his home, who is worried about the security of his smart home devices. Luca has less understanding of how to configure the smart devices. He asks the player to help him by searching devices and answering related questions. The player enters Luca's home by ringing the doorbell. There are five rooms in the house, each including two smart devices. Each time the player enters a

room, a mellow background music is played. The player should tap on each of the devices to display a question. For each question screen, there is also a hint button that helps the player to obtain supporting knowledge to answer the question. After submitting an answer, the game evaluates it and displays a notification. Eventually, the player is awarded based on the number of correct answers at the end of the game.

During the game, users have to answer ten questions where each question is aimed at one smart device. A number of factors were assessed for the selection of devices. It is essential to have a router in the home network. Since most devices are connected to the network via an app, we have considered choosing a smartphone as an intelligent device. We have also selected 6 devices (Smart TV, IP Camera, Smart Speaker, Smart Thermostat, Smart Lamp, Smart Plug) that most smart home owners are familiar with. To arouse the players' curiosity, the last two devices, Smart Home Firewall and Smart Mowing Robot, were chosen.

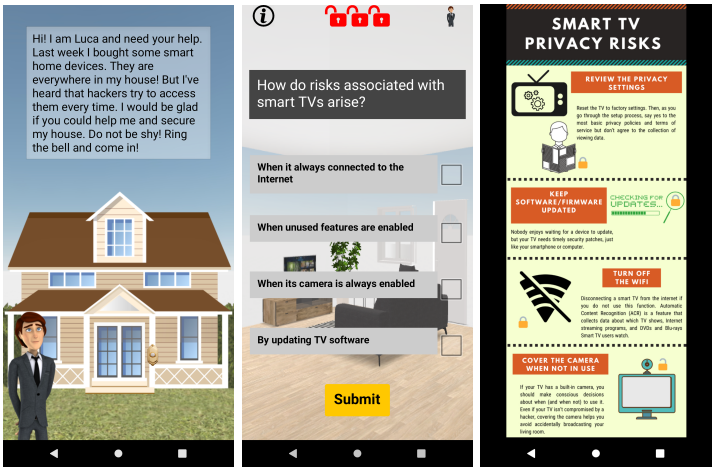

Fig. 1. The game helps players to get acquainted with security issues of smart home devices. Narrative (left), question (middle), and supporting knowledge screens (right).

3.1 Question Scenarios

The selected question for each device is based on the security and privacy concerns that have been addressed as threat models in research and articles in recent years [69, 58]. Consequently, 10 recommendations have been selected that are closer to the daily life of the users. Certainly, there is no doubt that the number of available recommendations is very large. However, all these items must be taken into account in the device settings. The following is an overview of the selected questions:

- *Router:* Setting up routers might be a tedious task for non-tech-savvy users. Although companies provide manuals, there is not enough information about the security issues caused by incorrect settings. Users have difficulties with understanding the configurations such as setting a secure admin password, choosing an appropriate protocol to encrypt the connection and utilizing technologies such as Wi-Fi Protected Setup (WPS) [36]. Consequently, the router question concerns which setup could help to have a secure router.
- *Smartphone:* Nowadays, smartphones are very popular and a convenient means of accessing and controlling smart home devices. Applications are being developed and are available for download from App Stores. The use of a fake, unofficial or outdated applications could lead to security problems for users' data and also for smart home devices [63]. Hence, we ask the players how an application could cause a security breach for smart devices.
- *Smart TV:* New generation of TVs integrate an operating system running multiple applications and an internet connection, allowing them to offer more services to users, however this might raise security concerns [4]. Webcam hacking, tracking problems and outdated software pose threats to user privacy [1]. In this scenario, users are encouraged to examine their understanding of these security and privacy issues.
- *IP Camera:* The IP cameras allow users to monitor their properties. It is easy to set up and does not require complex configuration. Users can also use an application to access the camera at any time and from anywhere. These functions are interesting for hackers. Various types of security attacks on the internet have become a serious threat to the video stream from IP cameras [17]. Therefore, users are advised to configure a variety of security recommendations, such as camera passwords, use of up-to-date applications and video encryption to protect against these threats [2]. This question investigates whether users understand the basic settings of a secured IP camera.
- *Smart Speaker:* It is easy to neglect that intelligent assistants are designed to be at the heart of smart home systems. While they allow users to surf the Internet, they can communicate and control other internet-enabled technologies at home. Recently, it was discovered that one type of attack allows hackers to secretly communicate with your device via white noise or YouTube videos - so they can send text messages or open malicious websites without the owners knowing [12]. Providing users with information about such harmful attacks helps them to protect their voice assistants from being attacked unwanted.
- *Smart Thermostat:* Controlling the smart thermostat via apps on smartphones allow the users to raise or lower the temperature remotely. The smart thermostats could create a gap in privacy and security of smart home networks, precisely because they learn about your habits and behaviour. Hackers could attack the vulnerable thermostat and get information about when users are not home, so they know when to break in without worrying about

[1] https://us.norton.com/internetsecurity-iot-smart-tvs-and-risk.html
[2] https://www.consumer.ftc.gov/articles/0382-using-ip-cameras-safely

users returning [26]. Such complex scenarios should be deeply understandable to users in order to protect their information and properties from attackers. The aim of this question is to inform users about the risks if someone gaining access to a smart thermostat.

- *Smart Lamp:* By connecting a smart lamp to the home network, users can control the brightness and sometimes change the color of the light from their smartphone. This provides more advanced features such as connecting the lamp to an alarm clock or flickering the desk lamp when new messages are received. These facilities are sometimes associated with security problems that could cause health and financial damages [51]. The purpose of this question is to provide users with recommendations to improve their knowledge to better decide how to purchase a suitable and secure intelligent lamp.
- *Smart Plug:* Smart plugs with cloud connection enable users to monitor and control electronic household appliances from anywhere. To manage them over the Internet, users should have a cloud account on the manufacturer's website or application and register the smart plug devices in the cloud service. However, they may suffer from insecure communication protocols and lack of device authentication [44]. With this question, we investigate the player's knowledge about user profile creation and understanding why the authentication and authorization of smart plug on the cloud server is important.
- *Smart Home Firewall:* By connecting smart devices to each other and to the Internet, smart home applications automate complex household tasks. Keeping track of the actions performed and controlling data communication could be confusing for inexperienced users. Rules for firewalls help protect the home network from malicious attacks as well as controlling the security vulnerabilities [65]. In this scenario, we encourage players to consider getting familiar with the firewall and the role of using them in smart home networks.
- *Smart Mowing Robot:* Mowing robots are becoming increasingly intelligent. They use GPS information to calculate the desired location and have an internet connection that enables them to communicate with cloud services and their applications. This scenario examines the advantages of using VPN when the user is away from home and wants to access the home network via a public Wi-Fi hotspot to take control of the smart mowing robot [49].

3.2 Game Procedure

The game consists primarily of the following building blocks:

- Finding devices: Players should find two devices in each room and answer the following questions regarding these.
- Request help: During the game, players may lack background knowledge to answer the questions. This event gives users insights about the context of the smart device and related security issues.
- Feedback of answers: After the player submits an answer, the game displays the result. If the answer was wrong, the player will receive the correct answer.

After starting a game session, the avatar will be displayed, expressing his goal via a textual speech bubble. By tapping on the doorbell, the player goes to the next state of the game (see Figure 1).

Question: Once the player enters a room, there are two available smart devices. By clicking on one of them, the question screen will be shown. All questions are multiple choice and the game informs the players while choosing the first device. On the top of the question screen, the player finds two buttons: The hint button on the left displays the supporting knowledge about the device's security, while the avatar icon on the right explains general game controls (see Figure 1). The player is directed to proceed to the next room after answering two questions.

Progression: Each play-through consists of 10 questions. Luca's home will become more secure, proportional to the number of correct answers. In order to transfer this concept to the player, 3 open red locks are displayed at the start of the game. Each of these locks turns into green closed locks after three correct answers given by the player. With 9 correct answers the player could get 3 green closed locks.

Supporting knowledge: By clicking on the information icon, the player is directed to the supporting knowledge screen. For the comparison of using text and infographics regarding their effect on player's motivation and performance, either text or infographics are displayed (see Figure 2). The content provided for the supporting knowledge is exactly the same for both versions. Every question includes a different supporting knowledge, separated from other questions. As for the used infographics, Various symbols have been added to transfer the concepts to the players and to increase their attention. A caption was selected for each infographic based on the associated device. For every device, we also designed symbols that convey basic concepts about device configuration or physical forms. To express the concept of being secure and insecure, there is a closed or open lock icon next to the titles or symbols. These concepts were applied to all infographics. The backyard is considered as the last room. By answering the two related questions, the player is directed to the reward interface where the number of correct answers and the corresponding reward are displayed on the screen.

4 Evaluation

To evaluate our research question, we conducted a between-subjects design user study with 60 participants. Within the first group (Text-Group), we evaluated with ($n = 30$) participants, using descriptive textual background information in the supporting knowledge screen. The second group (Infographics-Group) contained also ($n = 30$) participants, mutually excluded from the first, and introduced infographics instead of text in the supporting knowledge screen. We conducted laboratory study sessions on the university campus, with one participant per session and a duration of 30 to 45 minutes. As a mobile device, we provided a Google Pixel 2 XL with Android 9.0.

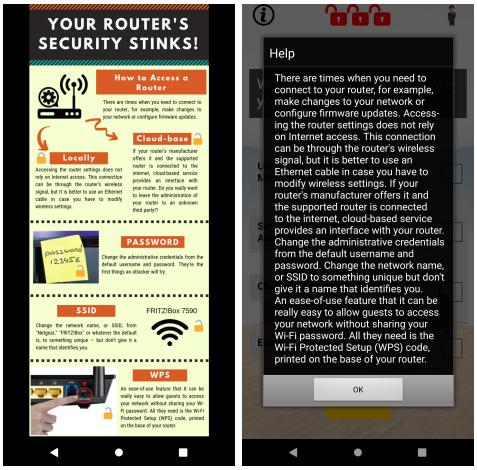

Fig. 2. Supporting knowledge screen: Infographics (left) and Text (right).

1. The interviewer provided an introduction about the game and security problems about smart home devices to the player.
2. The player ran the game, entered the rooms and answered related questions. Play time was measured.
3. After the game was over, the player answered a number of questionnaires.
   (a) The first questionnaire contained general questions regarding demographic information (e.g. age and gender).
   (b) In order to measure the usability of the game, the second questionnaire consisted of the System Usability Scale (SUS) [10].
   (c) Motivation of the player was measured by utilizing the Intrinsic Motivation Inventory (IMI) [48] on a 7 point Likert-scale.
   (d) Beside standard questionnaires, we had a number of self-designed context questions. The purpose of these questions was to understand the backgrounds of the players and their familiarity with smart devices.

4.1 Participants

A quota sampling approach was used to recruit participants for this study in which the selection was based on mailing lists, social networks, word-of-mouth and looking for users of smart home devices. Participation was voluntary and uncompensated. The first group consisted of 30 participants, 9 participants had a college degree, while 21 completed high school. Among the subjects, 15 people identified themselves as male and 15 as female. In terms of age, participants ranged between 18 to 54 years with an average age of 28.9 ($SD = 10.25$). The second group consisted of 30 participants, 14 participants had a college degree, while 16 completed high school. Among the subjects, 15 people identified themselves as male and 15 as female. In terms of age, participants ranged between 21 to 44 years with an average age of 30.6 ($SD = 6.38$).

5 Results

Statistical analysis was applied to identify possible differences between the two groups. To determine the impact of infographics on the players, the data from both groups were compared to each other.

After playing the game, participants were also asked to select all the smart home devices they own to see which devices are most commonly used amongst them. It turned out that all participants in the Text-Group owned at least one smart device in their homes and all of them had a smartphone. Table 1 shows an overview of the smart devices owned by the participants in the Text-Group.

Table 1. The number of smart devices owned by the participants in both groups

	Number of Devices	
	Text-Group	Infographics-Group
Smart TV	25	29
Smart Lamp	12	10
Smart Speaker	9	10
Smart Plug	3	2
IP Camera	2	3
Smart Thermostat	2	1
Smart Mowing Robot	0	0
Smart Firewall	0	0

The calculated mean value of SUS score for the Text-Group was 89.9 ($N = 30$, $SD = 14.70$). The IMI score of *Interest-Enjoyment* was rated 6.2 ($SD = 0.78$), *Perceived Competence* score was rated 3.4 ($SD = 0.1$) and *Effort-Importance* score was rated 5.6 ($SD = 0.97$). The average of correct answers was 2.4 ($SD = 0.17$) and the average play time was 9.27 minutes ($SD = 1.36$).

In the Infographics-Group, participants were also asked to select all the smart home devices they own. The results showed that all participants in this group also owned at least one smart device in their homes and had smartphones (see Table 1).

The calculated mean value of SUS score for this group was 84.0 ($N = 30$, $SD = 7.32$). The IMI score of *Interest-Enjoyment* was rated 6.0 ($SD = 0.65$), *Perceived Competence* score was rated 5.8 ($SD = 0.39$) and *Effort-Importance* score was rated 5.6 ($SD = 0.84$). The average of correct answers was 7.3 ($SD = 0.15$) and the average play time was 14.77 minutes ($SD = 2.89$).

The independent student's t-Tests [64] revealed that the participants in the Infographics-Group ($M = 7.3, SD = 1.15$) who received supporting knowledge in the form of infographics demonstrated significantly better average of correct answers ($t(58) = 11.734, p < .001, Cohen'sd = 3.030$) compared to the Text-Group participants ($M = 2.4, SD = 1.70$) (see Figure 3).

For average of playing time between two groups, the independent t-tests indicated that Infographics-Group participants ($M = 14.77, SD = 2.89$) showed a significantly higher average playing time ($t(58) = 9.441, p < .001, Cohen'sd = 2.438$) compared to the Text-Group participants ($M = 9.27, SD = 1.36$) (see Figure 3).

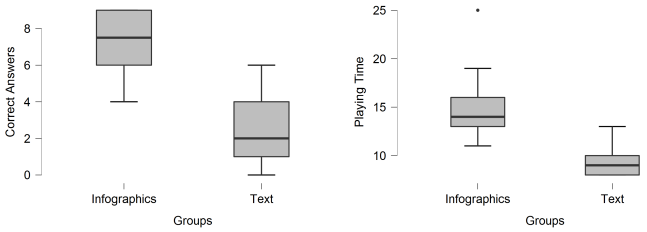

Fig. 3. The number of correct answers (left) playing time (right).

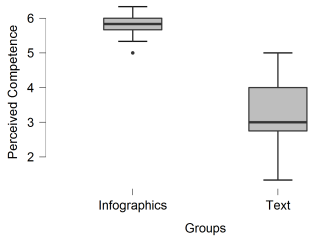

Fig. 4. The score of IMI test (Perceived Competence).

For IMI's *Perceived Competence* scores, independent t-Tests showed that the Infographics-Group ($M = 5.8, SD = 0.39$) significantly outperformed ($t(58) = 12.456, p < .001, Cohen'sd = 3.216$) the Text-Group ($M = 3.4, SD = 0.1$) (see Figure 4). We did not witness any significant differences in *Interest-Enjoyment* ($t(58) = 1.317, p = .193$), and *Effort-Importance* ($t(58) = 0.237, p = .814$) of IMI between the two groups.

Also, no significant differences in the SUS scores ($t(58) = 1.364, p = .178$) between the two groups could be found.

6 Discussion & Limitations

The purpose of this study was to investigate how a particular style of feedback, in this case infographics, affects the performance of edu-game players in the context of smart home security. Ultimately, the aim of this experiment was to provide answers to the comprehensive question: *To what extent can infographics as supporting knowledge improve the learning experience of users and make learning more effective in an educational game in a smart home security context?*

Results from the user study indicate that the game has a distinct usability and players enjoyed playing it, regardless of the difference in the form of supporting knowledge. Furthermore, our results showed high engagement towards the topic for the people who played the game. Participants were eager to spend time playing the game in both groups.

Players in the Infographics-Group answered significantly more questions correctly compared to the Text-Group. We evaluated that users performed better

when they got infographics as supporting knowledge. Due to high complexity of the topic, the questions could be considered as difficult for the average user. However, participants in the Infographics-Group performed reasonably well. This could indicate that using infographics as supporting knowledge could improve the performance of players in an edu-game even when the topic is rather difficult for the average user.

The resulting IMI *Perceived Competence* scores indicate that reading and viewing infographics considerably raise the players' confidence. The IMI (*Effort-Importance*) scores also show that the players made an effort to answer the questions in both groups. However, they were significantly less successful in terms of performance in the Text-Group. Even though participants were eager to answer the questions in both games, the infographics scored better. This could be evidence that not only a difference in motivation leads to the increase in correct answers, but the technical understanding was actually improved.

Although there was a significant difference in terms of (*Perceived Competence*), We did not witness any significant difference in terms of (*Interest-Enjoyment*) and (*Effort-Importance*) in the IMI results.

Nonetheless both groups rated very high absolute scores for these subgroups. This indicates that both versions managed to foster intrinsic motivation and raise players' interest and effort towards the topic regardless of the form of supporting knowledge.

Many of the game questions were selected from the security content which are available on web pages and users may read them throughout their daily life. It should be stressed that understanding the wording and sentences of questions could also affect the results. Based on performances of the players and their comments after the experiment, we found out that the difficulty of the questions were perceived differently between participants. Therefore, for the future we suggest to designing questions and creating levels based on complexity and difficulty of the topic. Users' playing time on average was observed significantly higher in the Infographics-Group than the Text-Group. One could argue that the difference in play time has an effect on the learning experience of the players. Although this might be true, nonetheless, it could indicate that the users would spend more time on the information if it's visualized with infographics rather than text which further will lead to a better learning experience. For future research, we suggest implementing a fixed time period for all conditions in which the player can access the supporting knowledge in order to focus more on the evaluation of the provided supporting knowledge and minimize other possible effects on the learning experience.

The game was characterized as a simple quiz-genre type, thus other game genres could be evaluated to extend the findings within different game genres. Our approach was aimed to help users gain more knowledge on how to make specific security decisions and raise their awareness towards smart home security issues. This knowledge can later help players to make more informed decisions while configuring and setting up their smart home environment. One should keep in mind that it is crucial for educational games in the context of privacy and

security to be updated regularly based on recent changes and updates to provide the latest information on the topic.

While these results present some significant steps forward in the investigation of using infographics as supporting knowledge in the context of smart home security, there are still some limitations that should be addressed. This experiment investigated how well a person performed in answering a question in an edu-game environment when they received two different feedback interventions. Although significant differences in performance between the conditions were found, there was no direct measurement of long-term learning after training. Furthermore, individual difference factors such as playing experience or learning type as well as the background knowledge can also lead to differences in players' performance. Although the question criteria used in this experiment were carefully calibrated from many research materials, they were limited to 10 items. It is possible that these criteria were still not specific enough. To understand the full impact of different approaches in game-based learning, future research needs to examine its potential effects in terms of alternative types of instructional support, as well as possible differential effects of timing (e.g., near real-time, delayed).

7 Conclusion & Future Work

This paper presents a novel approach to facilitate awareness and motivation as well as enhancing learning experience in an educational game by using infographics as supporting knowledge. We present a game that increases the intrinsic motivation of users and gives them more self-confidence in terms of the smart home security concerns. Our study shows that the adoption of infographics as supporting knowledge helps users to gain a better understanding of the complex context during the game and allows the players to produce a more engaging output. Our game has shown great potential in terms of usability and, according to most players, can be used to educate people about smart home security concerns. The extent to which users can remember the solutions and security recommendations remains a question for future work. Based on the results of this evaluation, we will attempt to assess the learnability of the topic through the game and the knowledge progress of the users by means of pre- and post-questions and additional smart home devices, questions and problems. The impact of the graphical elements used in the infographics for the purpose of privacy and security learning is also a topic for the future work.

8 Acknowledgement

This work was supported by the German Federal Ministry of Education and Research (BMBF) under the grant 16SV8503 (UsableSec@Home project).

References

1. Abawajy, J.: User preference of cyber security awareness delivery methods. Behav. Inf. Technol. **33**(3), 237–248 (Mar 2014). https://doi.org/10.1080/0144929X.2012.708787
2. Alotaibi, F., Furnell, S., Stengel, I., Papadaki, M.: A review of using gaming technology for cyber-security awareness. Int. J. Inf. Secur. Res.(IJISR) **6**(2), 660–666 (2016)
3. Arachchilage, N.A.G., Love, S., Beznosov, K.: Phishing threat avoidance behaviour: An empirical investigation. Computers in Human Behavior **60**, 185–197 (2016)
4. Bachy, Y., Nicomette, V., Kaâniche, M., Alata, E.: Smart-tv security: risk analysis and experiments on smart-tv communication channels. Journal of Computer Virology and Hacking Techniques **15**(1), 61–76 (2019)
5. Baddeley, A.D.: Human memory: Theory and practice. Psychology Press (1997)
6. Bahrini, M., Volkmar, G., Schmutte, J., Wenig, N., Sohr, K., Malaka, R.: Make my phone secure!: Using gamification for mobile security settings. In: Proceedings of Mensch Und Computer 2019. pp. 299–308. MuC'19, ACM, New York, NY, USA (2019). https://doi.org/10.1145/3340764.3340775
7. Bateman, S., Mandryk, R.L., Gutwin, C., Genest, A., McDine, D., Brooks, C.: Useful junk?: The effects of visual embellishment on comprehension and memorability of charts. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 2573–2582. CHI '10, ACM, New York, NY, USA (2010). https://doi.org/10.1145/1753326.1753716
8. Bellato, N.: Infographics: A visual link to learning. ELearn **2013**(12) (Dec 2013). https://doi.org/10.1145/2556598.2556269
9. Borkin, M.A., Vo, A.A., Bylinskii, Z., Isola, P., Sunkavalli, S., Oliva, A., Pfister, H.: What makes a visualization memorable? IEEE Transactions on Visualization and Computer Graphics **19**(12), 2306–2315 (Dec 2013). https://doi.org/10.1109/TVCG.2013.234
10. Brooke, J.: Sus: a retrospective. Journal of usability studies **8**(2), 29–40 (2013)
11. Burgers, C., Eden, A., [van Engelenburg], M.D., Buningh, S.: How feedback boosts motivation and play in a brain-training game. Computers in Human Behavior **48**, 94 – 103 (2015). https://doi.org/https://doi.org/10.1016/j.chb.2015.01.038
12. Carlini, N., Mishra, P., Vaidya, T., Zhang, Y., Sherr, M., Shields, C., Wagner, D., Zhou, W.: Hidden voice commands. In: 25th USENIX Security Symposium (USENIX Security 16). pp. 513–530. USENIX Association, Austin, TX (Aug 2016), https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/carlini
13. Chang, C.Y., Hwang, G.J.: Trends in digital game-based learning in the mobile era: a systematic review of journal publications from 2007 to 2016. International Journal of Mobile Learning and Organisation **13**(1), 68–90 (2019)
14. Chen, T., Hammer, J., Dabbish, L.: Self-efficacy-based game design to encourage security behavior online. In: Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems. CHI EA '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3290607.3312935
15. Clark, J.M., Paivio, A.: Dual coding theory and education. Educational psychology review **3**(3), 149–210 (1991)
16. Club, D.P.: *Mini Metro*. Game [Windows] (November 2015), dinosaur Polo Club, Aotearoa, New Zeland.

17. Costin, A.: Security of cctv and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations. In: Proceedings of the 6th International Workshop on Trustworthy Embedded Devices. p. 45–54. TrustED '16, Association for Computing Machinery, New York, NY, USA (2016). https://doi.org/10.1145/2995289.2995290
18. Cuevas, H.M., Fiore, S.M., Oser, R.L.: Scaffolding cognitive and metacognitive processes in low verbal ability learners: Use of diagrams in computer-based training environments. Instructional Science **30**(6), 433–464 (Nov 2002). https://doi.org/10.1023/A:1020516301541
19. Culyba, S.: The Transformational Framework: A Process Tool for the Development of Transformational Games (9 2018). https://doi.org/10.1184/R1/7130594.v1
20. De Castell, S., Jenson, J.: Digital games for education: When meanings play. Intermédialités: Histoire et théorie des arts, des lettres et des techniques/Intermediality: History and Theory of the Arts, Literature and Technologies (9), 113–132 (2007)
21. Denning, T., Lerner, A., Shostack, A., Kohno, T.: Control-alt-hack: The design and evaluation of a card game for computer security awareness and education. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. p. 915–928. CCS '13, Association for Computing Machinery, New York, NY, USA (2013). https://doi.org/10.1145/2508859.2516753
22. Deterding, S., Dixon, D., Khaled, R., Nacke, L.: From game design elements to gamefulness: Defining "gamification". In: Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments. pp. 9–15. MindTrek '11, ACM, New York, NY, USA (2011). https://doi.org/10.1145/2181037.2181040
23. Dixon, M., Gamagedara Arachchilage, N.A., Nicholson, J.: Engaging users with educational games: The case of phishing. In: Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems. CHI EA '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3290607.3313026
24. Dreams, D.: *Metrico+*. Game [Windows] (August 2016), digital Dreams, Utrecht ,Netherlands
25. Fiorella, L., Vogel-Walcutt, J., Schatz, S.: Applying the modality principle to real-time feedback and the acquisition of higher-order cognitive skills. Educational Technology Research and Development **60**, 223–238 (04 2012). https://doi.org/10.1007/s11423-011-9218-1
26. Fu, K., Kohno, T., Lopresti, D., Mynatt, E., Nahrstedt, K., Patel, S., Richardson, D., Zorn, B.: Safety, security, and privacy threats posed by accelerating trends in the internet of things. Computing Community Consortium (CCC) Technical Report **29**(3) (2017)
27. Fuchs, M., Fizek, S., Ruffino, P., Schrape, N.: Rethinking gamification. meson press (2015)
28. Georgiev, T., Georgieva, E., Smrikarov, A.: M-learning: A new stage of e-learning. In: Proceedings of the 5th International Conference on Computer Systems and Technologies. pp. 1–5. CompSysTech '04, ACM, New York, NY, USA (2004). https://doi.org/10.1145/1050330.1050437
29. Giannakas, F., Kambourakis, G., Gritzalis, S.: Cyberaware: A mobile game-based app for cybersecurity education and awareness. In: 2015 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL). pp. 54–58 (2015)

30. de Haan, Y., Kruikemeier, S., Lecheler, S., Smit, G., van der Nat, R.: When does an infographic say more than a thousand words? Journalism Studies **19**(9), 1293–1312 (2018). https://doi.org/10.1080/1461670X.2016.1267592
31. Heintz, S., Law, E.L.C.: Digital educational games: Methodologies for evaluating the impact of game type. ACM Trans. Comput.-Hum. Interact. **25**(2) (Apr 2018). https://doi.org/10.1145/3177881
32. Hendrix, M., Al-Sherbaz, A., Bloom, V.: Game based cyber security training: are serious games suitable for cyber security training? International Journal of Serious Games **3**(1) (2016)
33. Huang, W., Tan, C.L.: A system for understanding imaged infographics and its applications. In: Proceedings of the 2007 ACM Symposium on Document Engineering. p. 9–18. DocEng '07, Association for Computing Machinery, New York, NY, USA (2007). https://doi.org/10.1145/1284420.1284427
34. Hwang, G.J., Wu, P.H.: Advancements and trends in digital game-based learning research: a review of publications in selected journals from 2001 to 2010. British Journal of Educational Technology **43**(1), E6–E10 (2012). https://doi.org/10.1111/j.1467-8535.2011.01242.x
35. Johnson, C., Bailey, S., Buskirk, W.: Designing Effective Feedback Messages in Serious Games and Simulations: A Research Review, pp. 119–140 (11 2017). https://doi.org/10.1007/978-3-319-39298-1_7
36. Kaaz, K.J., Hoffer, A., Saeidi, M., Sarma, A., Bobba, R.B.: Understanding user perceptions of privacy, and configuration challenges in home automation. In: 2017 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC). pp. 297–301 (2017)
37. Kappen, D.L., Mirza-Babaei, P., Nacke, L.E.: Gamification through the application of motivational affordances for physical activity technology. In: Proceedings of the Annual Symposium on Computer-Human Interaction in Play. pp. 5–18. CHI PLAY '17, ACM, New York, NY, USA (2017). https://doi.org/10.1145/3116595.3116604
38. Karoui, A., Marfisi-Schottman, I., George, S.: A nested design approach for mobile learning games. In: Proceedings of the 16th World Conference on Mobile and Contextual Learning. mLearn 2017, Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3136907.3136923
39. Kay, M., Terry, M.: Textured agreements: Re-envisioning electronic consent. In: Proceedings of the Sixth Symposium on Usable Privacy and Security. SOUPS '10, Association for Computing Machinery, New York, NY, USA (2010). https://doi.org/10.1145/1837110.1837127
40. Knijnenburg, B., Cherry, D.: Comics as a medium for privacy notices. In: Twelfth Symposium on Usable Privacy and Security (SOUPS 2016). USENIX Association, Denver, CO (Jun 2016), https://www.usenix.org/conference/soups2016/workshop-program/wfpn/presentation/knijnenburg
41. Lankow, J., Ritchie, J., Crooks, R.: Infographics: The power of visual storytelling. John Wiley & Sons (2012)
42. Levie, W.H., Lentz, R.: Effects of text illustrations: A review of research. Ectj **30**(4), 195–232 (1982)
43. Linehan, C., Kirman, B., Lawson, S., Chan, G.: Practical, appropriate, empirically-validated guidelines for designing educational games. In: Proceedings of the SIGCHI conference on human factors in computing systems. pp. 1979–1988 (2011)
44. Ling, Z., Luo, J., Xu, Y., Gao, C., Wu, K., Fu, X.: Security vulnerabilities of internet of things: A case study of the smart plug system. IEEE Internet of Things Journal **4**(6), 1899–1909 (2017)

45. Lyra, K.T., Isotani, S., Reis, R.C.D., Marques, L.B., Pedro, L.Z., Jaques, P.A., Bitencourt, I.I.: Infographics or graphics+text: Which material is best for robust learning? 2016 IEEE 16th International Conference on Advanced Learning Technologies (ICALT) (Jul 2016). https://doi.org/10.1109/icalt.2016.83
46. Mayer, R., Bove, W., Bryman, A., Mars, R., Tapangco, L.: When less is more: Meaningful learning from visual and verbal summaries of science textbook lessons. Journal of Educational Psychology **88**, 64–73 (03 1996). https://doi.org/10.1037/0022-0663.88.1.64
47. Mayer, R.E.: Multimedia Learning. Cambridge University Press, 2 edn. (2009). https://doi.org/10.1017/CBO9780511811678
48. McAuley, E., Duncan, T., Tammen, V.V.: Psychometric properties of the intrinsic motivation inventory in a competitive sport setting: A confirmatory factor analysis. Research quarterly for exercise and sport **60**(1), 48–58 (1989)
49. Molina, M.D., Gambino, A., Sundar, S.S.: Online privacy in public places: How do location, terms and conditions and vpn influence disclosure? In: Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems. CHI EA '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3290607.3312932
50. Moreno, R., Mayer, R.E.: Role of guidance, reflection, and interactivity in an agent-based multimedia game. Journal of educational psychology **97**(1), 117 (2005)
51. Morgner, P., Mattejat, S., Benenson, Z.: All your bulbs are belong to us: Investigating the current state of security in connected lighting systems. ArXiv **abs/1608.03732** (2016)
52. O'Rourke, E., Ballweber, C., Popovií, Z.: Hint systems may negatively impact performance in educational games. In: Proceedings of the First ACM Conference on Learning @ Scale Conference. p. 51–60. L@S '14, Association for Computing Machinery, New York, NY, USA (2014). https://doi.org/10.1145/2556325.2566248
53. Paivio, A.: Mental representations: A dual coding approach, vol. 9. Oxford University Press (1990)
54. Papastergiou, M.: Digital game-based learning in high school computer science education: Impact on educational effectiveness and student motivation. Computers & Education **52**(1), 1 – 12 (2009). https://doi.org/https://doi.org/10.1016/j.compedu.2008.06.004
55. Park, B., Flowerday, T., Brünken, R.: Cognitive and affective effects of seductive details in multimedia learning. Computers in Human Behavior **44**, 267 – 278 (2015). https://doi.org/https://doi.org/10.1016/j.chb.2014.10.061
56. Plass, J.L.: Handbook of Game-Based Learning. Mit Press (2020)
57. of Play Games, S.: *Lumino City*. Game [Windows] (December 2014), state of Play Games, London, United Kingdom
58. Schiefer, M.: Smart home definition and security threats. In: 2015 Ninth International Conference on IT Security Incident Management IT Forensics. pp. 114–118 (2015)
59. Serge, S.R., Priest, H.A., Durlach, P.J., Johnson, C.I.: The effects of static and adaptive performance feedback in game-based training. Computers in Human Behavior **29**(3), 1150 – 1158 (2013). https://doi.org/https://doi.org/10.1016/j.chb.2012.10.007
60. Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J., Nunge, E.: Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In: Proceedings of the 3rd symposium on Usable privacy and security. pp. 88–99 (2007)

61. Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J., Nunge, E.: Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. In: Proceedings of the 3rd Symposium on Usable Privacy and Security. p. 88–99. SOUPS '07, Association for Computing Machinery, New York, NY, USA (2007). https://doi.org/10.1145/1280680.1280692
62. Shute, V.: Focus on formative feedback. Review of Educational Research **78**, 153–189 (03 2008). https://doi.org/10.3102/0034654307313795
63. Sivaraman, V., Chan, D., Earl, D., Boreli, R.: Smart-phones attacking smart-homes. In: Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks. p. 195–200. WiSec '16, Association for Computing Machinery, New York, NY, USA (2016). https://doi.org/10.1145/2939918.2939925
64. Student: The probable error of a mean. Biometrika pp. 1–25 (1908)
65. ur Rehman, S., Gruhn, V.: An approach to secure smart homes in cyber-physical systems/internet-of-things. In: 2018 Fifth International Conference on Software Defined Systems (SDS). pp. 126–129 (2018)
66. Van Eck, R.: Building artificially intelligent learning games. In: Games and simulations in online learning: Research and development frameworks, pp. 271–307. IGI Global (2007)
67. Wen, Z.A., Lin, Z., Chen, R., Andersen, E.: What.hack: Engaging anti-phishing training through a role-playing phishing simulation game. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. CHI '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3290605.3300338
68. Zargham, N., Bahrini, M., Volkmar, G., Wenig, D., Sohr, K., Malaka, R.: What could go wrong? raising mobile privacy and security awareness through a decision-making game. In: Extended Abstracts of the Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts. p. 805–812. CHI PLAY '19 Extended Abstracts, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3341215.3356273
69. Zeng, E., Mare, S., Roesner, F.: End user security and privacy concerns with smart homes. In: Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017). pp. 65–80. USENIX Association, Santa Clara, CA (Jul 2017), https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng
70. Zichermann, G., Cunningham, C.: Gamification by design: Implementing game mechanics in web and mobile apps. " O'Reilly Media, Inc." (2011)