Information Security at Schools: A Practical Game-Based Application with Sustained Impact

Margit SCHOLL
Faculty of Business, Computing, Law, Technical University of Applied Sciences
Wildau, 15745, Germany

Regina SCHUKTOMOW
Faculty of Business, Computing, Law, Technical University of Applied Sciences
Wildau, 15745, Germany

ABSTRACT [1]

The process of awareness raising should be seen as an important factor in enhancing knowledge of information security issues and developing appropriate behavior in response to them. In the project described here, this is carried out by means of awareness training based on experience-oriented learning scenarios, coaching, and mentoring concepts. These have been partially modified or newly developed on the basis of previous projects, drawing on concrete everyday school situations, using appropriate language, and applying three different levels of difficulty. A total of about 600 pupils from five pilot schools in Berlin and Brandenburg are participating in this research project. In the classes involved, information events, online surveys, trainings, and creative workshops were offered.
Attempts are also being made to train teachers and provide parents with information to help ensure an ongoing impact in schools with long-term effects. Pupils were able to take the exam for the IT security module of the International Computer Driving License. One teacher per pilot school was able to take part in the very extensive training and certification to become an information security officer. After all the trainings and experience-oriented measures that have been carried out, it is clear that teachers have developed and implemented new teaching ideas, and that the important topic of information security has been made more understandable for pupils.

Keywords
Information Security, Security Awareness Training, Sensitization, Game-Based Learning

1. INTRODUCTION

The progress of information technology (IT) and information communication technology (ICT) has accelerated enormously over the last fifteen years. The world we live in is becoming smarter. We benefit from our new smart world, which is taking rapid steps forward. Information reaches us faster, and bookings and reservations can now be handled in a few minutes: we are all networked. Our lives are now permeated by digitization and its underlying processes, which are influenced by IT and ICT. We speak of digitization when the infrastructure of public and private space is improved [8]. Schools and the school system are also becoming smarter, although this varies from country to country. By 2014, 82 percent of German schools were using digital whiteboards [5], indicating that modern Internet-based learning was taking place in class, with content presented in digital form. Children and young people today seem to be more independent in their acquisition of knowledge because they can find answers to a wide variety of questions on their smartphones, thanks to the almost universal availability of the Internet. We all use web services and apps in the belief that the Internet is trustworthy. Yet the opposite is the case: the Internet is an untrustworthy network, and everyone needs to learn to be more aware of the hidden risks.

But what risks does digitization entail in daily life? Are adults and pupils aware that they are obliged to share their personal data when they use web services and apps? Can parents and teachers convey a nuanced picture of the threats, vulnerabilities, types of hazard, and possible extent of damage? Can they give specific help to children and teenagers? Do adults and pupils have enough knowledge about and sensitivity to the potential impact of thoughtless actions? How good is their knowledge of security and their actual behavior in this context? According to an online survey in the German “SecAware4school” project, more than half of the respondents in five pilot schools are interested in the topic of information security and would like to learn more about it. The results of the survey indicate that there are significant differences in the knowledge and user behavior of the respondents. Pupils should learn how to use digital media safely and independently, because nowadays children and young people are confronted with a large number of different media at an ever earlier age. Schools alone cannot meet

[1] We would like to thank Simon Cowper for his comprehensive and detailed peer-editing of this extended paper.

this challenge, since even teachers need to acquire skills in the field of information security. The research team deals with the topic of information security at schools within the project SecAware4school. The aim is to raise awareness among pupils, teachers, and parents in relation to the topic of information security.

This paper is based on the diverse and practically oriented experience of a research group that has been dealing with questions of awareness raising in various projects for a number of years and looking at other courses with a view to providing specific trainings that would increase awareness of information security and data protection. This paper is focused on raising awareness in daily school life and briefly summarizes previous findings in the second section. The third section shows the methodology, while the fourth section discusses the game-based learning concept. In order to illustrate the nature of the learning scenarios, some examples will be presented in the fifth section along with some comments. The sixth section summarizes important findings and points to future areas of focus.

2. RESEARCH PROJECT

The SecAware4school project was funded by the Horst Görtz Foundation (HGS) from September 2018 to August 2020. It set out to raise awareness among pupils, teachers, and parents on the topic of information security. The interests of the target groups and concrete everyday situations are foregrounded—making participants aware, for example, of the need to handle personal data consciously and carefully when using Internet services and social networks. The fundamental idea is to train young safety advisors from among the pupils at the five pilot schools, so that after the project, with the support of the teachers, they can use their knowledge and experience to pass on what they have learned to other pupils, especially in their own application of the experience-oriented game-based learning scenarios. It was assumed that at least 10 percent of the participating pupils would successfully complete a certification test after being explicitly trained, so that by the end of the project there would be sixty young security advisors. However, the Covid-19 pandemic reduced these expectations. Nevertheless, after the project, many of the pupils will also be able to share their knowledge and experience with pupils from other classes and schools as necessary. Another key idea was the focus on imparting basic technical and organizational knowledge about information security via experience-oriented analog learning scenarios combined with diversified coaching and mentoring concepts. Some cases were also being developed in the digital format. For the target group of pupils, this means that these learning scenarios must not only be adapted to the concrete everyday situations and language of the children and young people but must also be developed in modular form at three different levels of difficulty according to the three age groups defined at the pilot schools: sixth-, ninth-, and eleventh-grade level. At the end of the project, in December 2020, the pupils will have ten specific learning scenarios that meet their needs, each at three different levels of difficulty, making a total of thirty experience-oriented learning scenarios.

The project SecAware4school enabled a select group of fifteen teachers at the pilot schools to receive further training in the International Computer Driving License (ICDL) module content “IT Security” in line with the train-the-trainer concept and based on specific conditions, so that they in turn can prepare their pupils for the relevant exam themselves. However, the Covid-19 pandemic reduced these expectations, too. Nevertheless, the project enabled the pilot schools to implement a sustainable measure that allowed five teachers (one per pilot school) to complete a special, complex training over fifteen days and take the certification as information security officers free of charge. For this purpose, a handbook [2] was given to these teachers as the basis for the training. They were required to submit a practice-oriented project report and sit a final two-hour, computer-based examination with 120 questions. The five-year certificate as an information security officer is achieved if over 75 percent of the 120 questions are answered correctly. If further training in the area of information security is carried out during the five-year period of validity, then the certificate can be extended without the need for another examination. The project thus enables the pilot schools to achieve sustainable information security measures, which was previously not possible.

One of the biggest challenges in the project was the organization and scheduling with the pilot schools. Owing to a shortage of staff in German schools, teachers are given few opportunities to address the topic of information security—there are a great many other topics to focus on. This fact creates organizational challenges and makes communication with the schools more complicated. In addition, each of the participating classes must be visited several times by the project team, and these regular school lessons were sometimes canceled because of other school events. Moreover, creative workshops and awareness-raising trainings—which enable the implementation of the pupils’ own ideas and ensure a positive response—are time consuming. Despite the challenging conditions, the pilot schools on the project all agree that raising pupil awareness of the important topic of information security needs to be prioritized at schools.

3. METHODS

Game-based, accelerated, and authentic learning approaches will be combined to achieve the goals outlined above. In addition to being a varied and stimulating didactic form [17], game-based learning (GBL) enables pupils to focus on a set goal and provides them with direct

feedback [10]. Gamification means the interaction of playful learning and thinking, game mechanics, aesthetics, commitment, and the motivation to learn and act, amplify the learning process, and solve problems [15]. The three different requirement levels of the game-based learning scenarios promote the further development of the participants without asking too much of them [7]. Accelerated learning (AccL), on the other hand, requires the active creation of knowledge by pupils, beyond passive perception [3] [18] [20] [6]. This approach seeks to enable learners to internalize skills independently and with long-term effect. A combination of the two methods is applied in the SecAware4school project in the form of experience-oriented learning scenarios in everyday school life based on analog and digital games that provide motivation and generate a sense of emotional engagement. Authentic learning (AuL) focuses on the application of knowledge in real contexts and situations. The key here is to enable pupils to learn from experience, from real or simulated problems, thus creating a meaningful collective result. This is also necessary for team-based exchange on the subject of information security [21] and thus supports experiential learning in the scenarios.

The survey by Hamari et al. (2016) examined the impact of challenges and engaged involvement on learning [13]. It was found that the challenge of the game has a positive effect on learning, both directly and by increasing levels of engagement. The challenge that the game presents [13] is crucial to the learning effect. This is also supported by the practice of the three requirement levels of the SecAware4school project. Each level of requirement is precisely adapted to the particular class. In the digital learning scenario “Rights to Photos” and in the analog learning scenario “Information Security: Rapid Guessing” (see fig. 1), the majority of the classes participating in the project noticed that the pupils strive for a greater challenge and voluntarily try to reach higher levels in the learning scenario. This creates a positive learning effect. It is thus highly advantageous to create a game-based and adaptive learning environment in the classroom [13].

Awareness trainings (AT) are designed to actively allow participants to achieve real awareness through a process of emotional engagement and motivation. In our experience, this can be achieved very successfully with *analog* learning scenarios and verbal exchanges, even in the digital world, if the complexity of the topic can be reduced to accord with the needs of the specific target group. Originally developed for company employees [14] [4], ATs also appear to be extremely useful in schools as a means to raise awareness among pupils, teachers, and parents. In the participating pilot schools, ATs represent an unusual pedagogic approach that offers a contrast to frontal teaching. They should be seen as a first step in awareness raising. It is not just a matter of conveying knowledge, since simple knowledge transfer does not give people an emotional connection to the abstract topics of information security [4], which is exactly the point of the exercise. All the more interested and brighter pupils take part in the individual analog and digital learning stations. This leads to stimulating discussions and an exchange of views about content. There are various advantages to this, such as the promotion of skills in the areas of communication and cooperation, the forging of a connection with the real problems the pupils face, and the perceived reduction in complexity of challenging learning material. At the same time, the ATs are used as an opportunity to test the experience-oriented learning scenarios and, if necessary, to further develop and adapt them.

Fig. 1 Analog learning scenario “Information Security: Rapid Guessing” in action

If people have understood the meaning of ATs by practicing them themselves, they can suggest improvements to the experience-oriented scenarios or develop their own learning scenarios in creative workshops (CWs) with help from the project team. In the CWs, the participants are asked to make suggestions on how to adapt existing analog and digital experience-oriented learning scenarios in order to better reflect the problems and needs of their daily life. The ideas developed by the pupils and teachers are then implemented by the project team and given back to the target groups for testing. One teacher took advantage of the opportunity to elaborate his own analog learning scenario for his pupils, while another established a new one-year elective course in which pupils develop both analog and digital learning scenarios and can thus immediately implement the programming skills they have learned. This indicates in both cases that the teacher is highly motivated to give information security and experience-oriented learning methods a more sustainable footing in classroom activities.

Experience-based, game-based, and team-based learning scenarios as awareness-raising measures allow learners to make mistakes, experiment, and thus practice the right way of doing things [23]. Participants work toward a goal, choose and carry out actions, and experience the consequences directly. The advantage of these activities with young facilitators is that the transfer of knowledge by near-peers is often perceived as more credible and authentic than knowledge delivered by adults. The approach of the entire project offers further advantages such as the promotion of communication and cooperation skills, the connection with real problems from the pupils' lives, and a reduction in the complexity of challenging learning content.

4. GAME-BASED LEARNING CONCEPT

During development of the game-based learning concept, it is important to note that learners are motivated by different game elements and that structured gamification makes it possible to modify the game elements without changing the system or redesigning the learning content. Kapp (2013) and Stuart et al. (2019) identify three successful levels of gamification abstraction: motivation strategy, which includes rewards, time limits, and clear goals for learning progress; the game elements that contribute to implementation; and the game element instances that correspond to the context and learning profile [16][22]. These aspects were taken into account in the development and implementation of the game-based learning concept in the SecAware4school project.

The establishment of an elective course in one of the pilot schools based on selected methods from the research project has successfully led to pupils being made sensitive to information security. Although this one-year seminar is designed for grade 10, the degree of complexity can be adapted to any class level. The concept has been developed by the project team in cooperation with the teacher responsible for computer sciences in the pilot school. We recommend the following phases in the process of refining the content and implementing a seminar/course of this kind:

First Phase:
Creative Thinking Process
After an introduction to the topic of information security by the teacher and some AT sessions with the pupils using existing experience-oriented learning scenarios,[2] small working groups are formed. The teams are now tasked with developing a learning scenario for younger class levels, which makes them aware of how their own data is used. In the creative phase, the working groups have to explore the possible topic and assemble a range of different ideas. Methods such as design thinking in the creative workshop are suitable for this. In the creative thinking process, pupils and teachers are encouraged to make suggestions about how to adjust and improve existing analog and digital experience-based learning scenarios and develop ideas for new learning scenarios that reflect the problems and needs in their everyday lives (see fig. 2). The further development and generation of new learning scenarios with the help of various creative methods is intended to enable participants to better empathize with the moderation role later on and prepare them to develop new learning scenarios independently (at the end of the project).

Second Phase:
Conceiving and Developing the Idea
While developing a concept for the learning scenario, it is important to document the individual steps in order to establish a prototype for the learning scenario. Each of the students' small work groups should appoint a team coordinator—this is better than if the teacher takes on this role. The team coordinator is a driving force for the development of the learning scenario, moderating the group dialogues and documenting decisions. The teacher acts as a coach for all the individual student groups. In particular, the documentation of precisely perceived situations, group dynamics, interaction with team coordinators, and non-verbal communication promotes effective understanding of the goal of the learning scenario further down the line (see fig. 2).

Third Phase:
Evaluation of the Prototype
The developed prototype should be tested several times with different groups, especially with the defined target groups—in our experience, at least three iterations are necessary to obtain a finished learning scenario from the successively improved prototype by the end of the school year. It should be noted that digital learning scenarios also require good programming skills, while the analog learning scenarios can focus on the exchange processes within the target groups involved in the game (see fig. 2).

Fourth Phase:
Outcome
The final learning scenario is developed on the basis of a wide variety of exchanges within the students' development group, with the supervising teacher, and with the actual target groups. After these exchanges and the iterative improvements to the learning scenario, the development group (in our case, tenth-graders) is made aware of the topic and is clearly motivated to use their learning scenario. The pupils now act as multipliers in their school, and each time they use their learning scenario, they themselves gain greater competence in

[2] In December 2020, the pilot schools involved will receive a set of thirty-six learning scenarios at the end of the project. Other schools can borrow scenarios from the university or hire the project team.

moderating the topic, which can also be reflected in their private lives.

This way of establishing information security as a subject in schools increases pupil awareness in a playful and haptic or digital way. Pupils acquire knowledge through self-research, working in groups—which promotes social skills—and slipping into the role of trainers. This enables them to develop a ready-made learning scenario for ongoing use and to act as moderators, since this is where the train-the-trainer method is applied. In their learning scenarios, the older class levels help raise awareness among the younger pupils. When this takes place in the context of the regular curriculum, the pupils should be supported with qualitative input to guide and coach them as teachers. It is important for the work groups who have decided to program a digital learning scenario to be taught the necessary basics of programming and to receive intensive support in the process of software development.

Fig. 2 Steps in the development process (1 to 4) for the learning scenario "Security Surfer: Hazards and Protective Measures" devised by the project team

The literature review by Acquah & Katz (2020) shows six key game features highlighted within the studies on digital game-based learning tools that influenced the outcomes:

- ease of use
- challenge
- rewards and feedback
- control or autonomy
- goal-orientation
- interactivity [1]

The overall findings presented by Acquah & Katz (2020) show that digital game-based learning is an effective tool within schools. However, future research should explore how these findings can best be implemented in the classroom setting [1].

In their study of the learning progress and levels of motivation among Portuguese teenagers in the use of new media, Pereira et al. (2019) make the following observation: "The dissonance between what teenagers learn in classrooms and their everyday lives is not a recent phenomenon, but it is increasingly relevant as school systems are unable to follow the evolution of media and society beyond traditional concerns regarding the protection of young people." [19] This is why the SecAware4-school project uses a combination of game-based, accelerated, and authentic learning approaches to achieve the project's goals.

The main research results of Pereira et al. (2019) confirm the existence of a gap between formal and informal education in different respects. First, informal education is primarily motivated by the needs and peer influence of the teenager [19]. This confirms the approach taken in our project, whereby the active participation of pupils in the development of their own learning scenario is of great importance. Pupils moderate their learning scenarios for and with other young target groups. Second, colleagues and family appear—alongside the Internet and self-discovery—to be important sources of knowledge [19]. This corroborates our strategy of educating and informing the pupils' caregivers (teachers and parents) about information security. Third, a teenager's informal learning contributes to the development of skills and competencies that are also useful from a school point of view [19]. Conversely, it means that schools should specifically promote such informal learning arrangements, as our project has shown.

In addition, our project suggests that the successful and modern activation of information security awareness has been positively tested by the method of gamification. It is of great importance for society and for the future to prepare children, pupils, and young people for the smart, digital world and to train them in information security awareness. For implementation to be successful, everyone, both government and society, must pull together to counter the threats posed by digital crime. The possibility of successfully implementing and establishing information security as a topic and course component has been illustrated in the SecAware4school project.

5. PRACTICAL EXAMPLES: SELECTED LEARNING SCENARIOS

At the beginning of each learning scenario, the playing time must be agreed in cases where the players do not want to play according to the time recommended in the instructions. In every learning scenario, a warm-up is necessary to get the participants in the right mood for the scenario.

In some of the scenarios, it is assumed that a moderator who does not play the game himself will be appointed.

This must also be clarified before the game starts. In general, it is advisable to appoint a person in each learning scenario to explain the rules, keep track of the playing time, and point out the correct answers.

Information Security: Rapid Guessing (Analog)
In the learning scenario "Information Security: Rapid Guessing," the use of technical terms in the field of information security is practiced. The increasing availability of information and services online means that it is important to become familiar with the technical terms relating to information security.

The aim of the learning scenario is for players to guess technical terms according to the "Hangman" principle by means of hints. The players have about 15 minutes to work through the pile of cards at their level of difficulty. Only three failed attempts are allowed per card. An excerpt from an awareness training is shown in figure 3. This scenario can be played by three or more people—either in two teams (at least one person per team plus one moderator) or a team plus a moderator. The playing time is approximately 15–25 minutes.

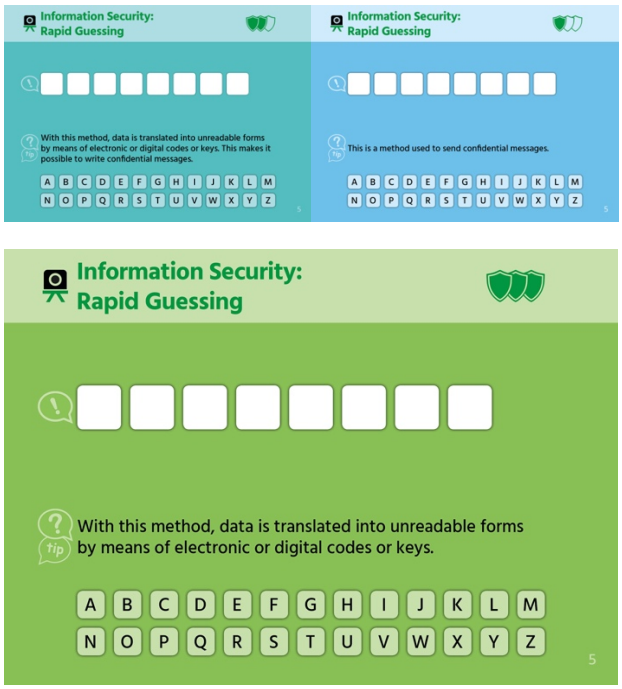

Fig. 3 Learning Scenario "Information Security: Rapid Guessing"—available in three levels of difficulty (in English and German)

Online Behavior (Analog)
The aim of this learning station is to find team solutions for different online situations, and to identify appropriate and well-thought-out ways of making people aware of how to interact on social media. "Treat others as you would like to be treated yourself!" This golden rule applies both in the real world and on social media. The participants should become aware of potential security issues and risks on social media and in everyday school life and be able to identify and take appropriate protective measures. In this context, topics of information security were also addressed, including physical aspects of the issue. Warm-up questions in this scenario include:

- "Are you familiar with situations (on social media) in which it is easy for sensitive information to be disclosed?"
- "Have you ever noticed that someone is being bullied on social media?"
- "How many apps do you use for social networking?"
- "Do you pay attention to the correct spelling and tone while chatting on social media?"

"Online Behavior" includes the following components: playing field (see fig. 4), question cards, case cards, term cards, two playing figures, four chips, an hourglass, and the dice. After deciding on a moderator, the duration, level of difficulty, and the division into teams, team A starts by rolling the dice. The symbol on the dice indicates the category to be played for. The explanation of the category cards in the instructions must be read before the card is removed from the stack. The team must discuss and jointly decide on an answer within one minute. The chips are used to mark the allocation while the move is being made on the playing field. The moderator provides the answer based on the model solution. If an answer does not correspond to the model solution but was justified in a comprehensible manner, the moderator can apply points for this: what is most important here is for the participants to reflect. If the team has given the correct answer, it may move to the next field. If the answer is wrong, the team must remain where they are. Then it is the turn of the next team.

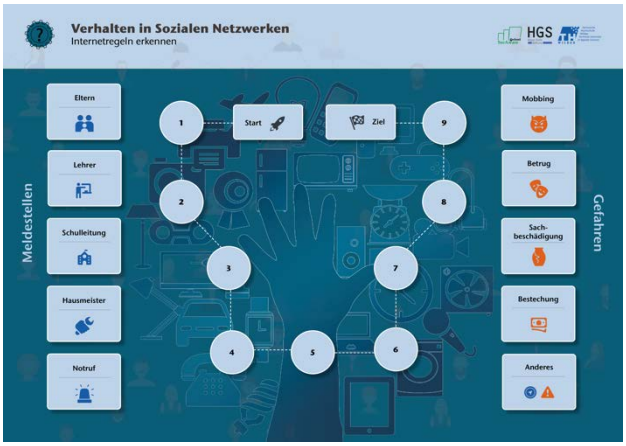

Fig. 4 Learning Scenario "Online Behavior"—available in three levels of difficulty (in German)

The category cards are to be understood as follows:

- *Case – Act correctly!* In order to succeed at this task, choose a player from your team to read a statement out loud. The hourglass is then turned over and you must consult with the rest of your team and map the case to a category and the correct contact person (parents, teachers, school management, emergency

services, support helpline, counselor) within one minute.

- *Question – Answer cards* Here an example (a question) on social media is given: to complete this task successfully, choose a player from your team to read a question out loud about social media. They then take a card from the stack and turn over the hourglass. The team must respond within one minute.
- *Term – Explain cards* The term has to be explained without using the related words. Choose a player from your team to explain a term to the team. No words may be used that are not shown on the card. The team has to try to guess the term. The opposing team checks that the terms are used correctly. The person who has been selected takes a card and prepares briefly before the hourglass is turned over.

Storytelling in Information Security (Analog)

The aim of the learning scenario is to explore basic concepts of information security and become familiar with the topic. The learning scenario "Storytelling in Information Security" (see fig. 5) involves creating a short story based on a specific information security topic and incorporating the symbols on the dice into the story. The story can be funny, serious, or offbeat. There are no limits to the imagination. The important thing is that all the symbols on the dice are included and are made relevant to the theme. The serious game "Storytelling in Information Security" includes the following components: white-boards, whiteboard marker, six dice with different icons, and six themed cards.

Fig. 5 Learning scenario "Storytelling in Information Security" (analog)—available in three levels of difficulty

The game starts with each team drawing a card from the pack at the correct level. This card now provides the topic about which a story must be invented. First of all, the term in question should be clarified. Then the moderator reads the corresponding explanation from the instructions. The six dice are then thrown all in one go. The icons appearing on the dice apply to both teams. The task of each team is now to concoct a story about the topic that incorporates the symbols on the dice. The participants use the mini-whiteboard to write down the story. The game ends after the agreed playing time. The teams then read the stories to each other and discuss whether all the symbols have been incorporated and if the story is matched to the topic. Teams score points for the theme and each correctly used icon. The moderator adjudicates any dubious situations. The story can be photographed and presented later in class.

The digital version of "storytelling" is consistent with the analog learning scenario (see fig. 6). The learning scenario is ideal for deepening and repeating basic concepts of information security. The digital learning scenario promotes independent learning individually and in teams. Players can work together at school (e.g., in the computer room), on the road with their smartphone/tablet, or from home. The digital version can be used across classes regardless of age. This learning scenario is not restricted to the topic of information security and can be adapted to any subject. The SecAware4school project focuses on the topic of information security.

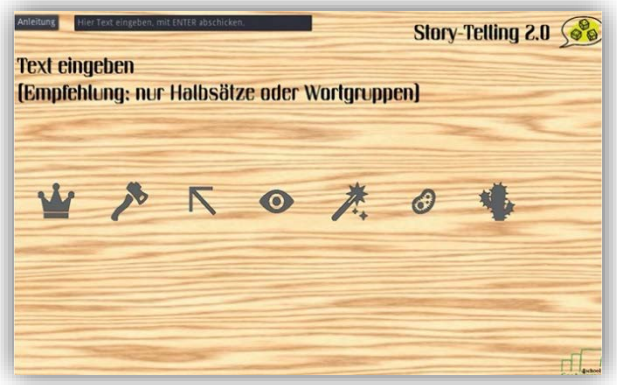

Fig. 6 Learning scenario "Storytelling in Information Security" (digital)

Fake or Real? (Analog)

This learning scenario focuses on the individual filtering mechanisms involved in the reception of information. It demonstrates the existence of misinformation within the media and the diverse risks this poses to students and young people. The aim of the scenario is for students to eliminate the falsehoods on the cards and to recognize the fake news cards, thus sharpening their awareness of its characteristic features.

The components include squares of red and green felt, 16 message cards, the golden-rule card and the definition card. The cards relating to the difficulty level that has been selected are placed face down on the table along with the felt squares. The participants may sit around a table (see fig. 7). The moderator gives the introduction and imparts

important information from the guidelines. It is important for players to pay close attention to the moderator's text. The game mechanics are based on the assignment principle and are intended to stimulate discussion among the participants. The general task is to decide which news items are true and which are fake.
For each decision, players are given about 20 seconds per card. In our opinion, this is in line with the fact that people no longer perceive the abundance of information they are exposed to correctly and must decide for or against a particular item of news within the first few seconds of encountering it. The participants receive the golden-rule card during the evaluation and should use it to justify and correct their decisions. After the playing time is over, players can perform a follow-up task that involves generating a discussion with prepared questions from the instruction guide.

Fig. 7 Learning scenario "Fake or real?" (analog): stories in German and available in three levels of difficulty

Security Duel (Analog)
The learning scenario "Security Duel: Information Security in the Company" was developed as a means to familiarize students with a particular company structure in connection with the use of IT security measures. The pupils learn about the security measures that organizations can use to protect their sensitive information and IT infrastructure. The three levels of difficulty differ in the frequency with which unfamiliar terms need to be consulted in a specially developed reference book (Wiki). This learning scenario is especially relevant for grades 8 to 11.

The playing field (see fig. 8) shows different areas of a company that must be protected from attackers. Attacks and subsequent defensive actions are carried out alternately by two teams. The task of the defense team is to protect the different areas of the company (e.g., customer database, network, human resources department) as much as possible from the attackers using adapted protective measures (e.g., social engineering/information security officer training). The attackers' team has the task of finding weak points in the company's departments and gaining access to sensitive data.

The components in "Security Duel" are as follows: playing field, 29 attack cards, 29 defense cards, 20 yellow and 20 blue figures, playing chips, dice, and Wiki, which includes descriptions of difficult terms. One turn always consists of an attack-defense action. Depending on the level of difficulty, the participants have the option of looking up unknown terms in the Wiki. Examples are as follows:

- Attack: Team A takes two cards from the attack stack and must decide which area of the company they want to attack. Then they should place the card face up on the selected field and justify their move.
- Defense: Team B takes three cards from the defense stack and decide which of the three cards they want to use to protect themselves against the attack and place the card face up on the field that has been attacked—they then justify their move.

The moderator supplies the correct answer and awards the points. The winning team places one of their color figures on the field that has been played. After an attack-defense action, the teams switch roles. Team B attacks and team A defends.

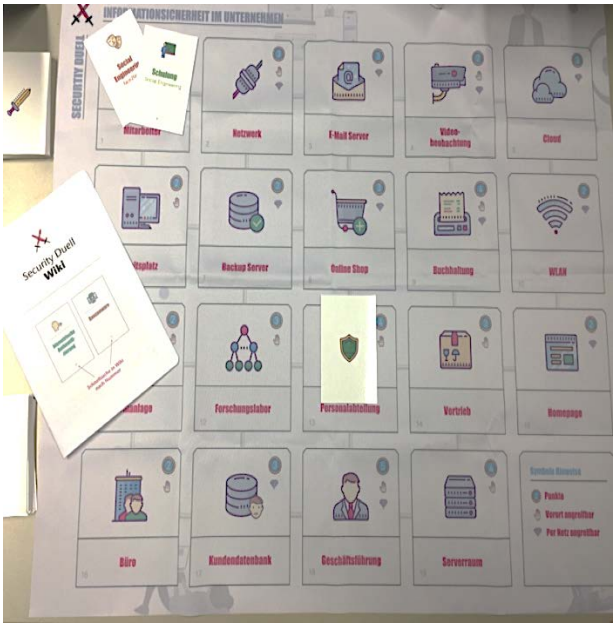

Fig. 8 Security Duel (analog)—available in three levels of difficulty

Sketch–Secure Passwords (Digital)
This learning scenario is ideal for deepening and repeating basic knowledge of password security. "Security Sketch" promotes independent learning and shows the mistakes that can be made with passwords and the correct procedures for handling them. The digital scenario can be played at school (e.g., in the computer room), on the road with the smartphone/tablet, or from home. The "Secure Passwords" scenario can be used across classes regardless of age. Adopting the role of "Ms. Hackermann" the player must make the right decisions about password security (see fig. 9). For example, a decision needs to be made

about how to deal with a new password and if/where this is noted. The goal is to ensure the correct handling of passwords.

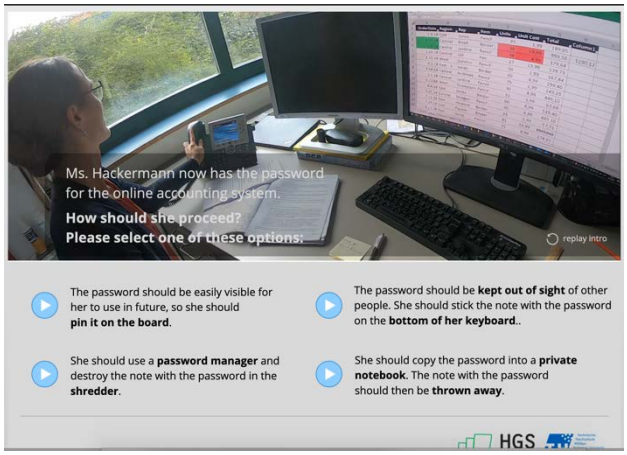

Fig. 9 Interactive video-based learning scenario "Sketch–Secure Passwords" (digital)

Image Rights (Digital)

This learning scenario helps in dealing with the topic of image rights. The generally careless handling of multimedia content raises numerous questions. Raising participant awareness should help foster future behavior that is legally compliant. The questions are presented as a quiz with many practical examples at three levels of difficulty. A comparative evaluation of the team's correct and incorrect answers provides information on the degree to which the topic is already anchored in the minds of the participants. The focus of this digital learning scenario is on copyright, source attribution, and the legally compliant handling of multimedia content in general and image material in particular.

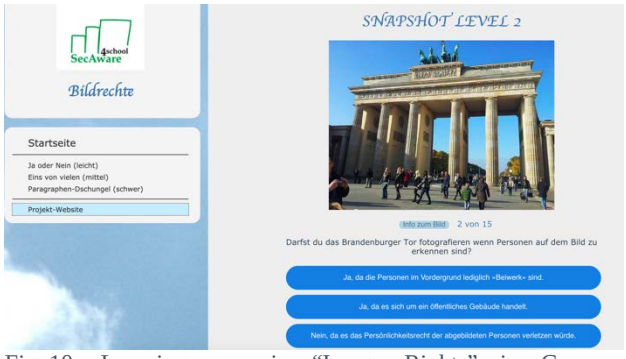

Fig. 10 Learning scenario "Image Rights" in German (digital)—available in three levels of difficulty

Security Surfer: Hazards and Protective Measures

This learning scenario addresses the global topic of the Internet. The hazardous waters of the Internet are examined in more detail. As you surf through its vast ocean, it is important to recognize the dangers and identify the appropriate protective measures.

The goal of the "Security Surfer" scenario is to surf the World Wide Web between the islands, to recognize the possible dangers and to find appropriate protective measures. There are a total of six islands that you must protect from danger. Each island symbolizes an area of the Internet and is composed of a different number of sub-islands. The aim is to protect the islands by responding to questions about safe surfing on the Internet and finding appropriate protective measures. It is important to develop a strategy to protect as many islands as possible.

The components of the scenario include a playing field, 18 questions cards at three levels, 6 phishing cards, 4 figures and 40 pins in 4 colors. After the playing time has been agreed, teams are formed, and the appropriate level is selected. All question cards must be placed face down on the wave symbols of the playing field (see fig. 11). One of the teams starts by placing the figure on the next playing field, before reading the card out loud and answering the question. The moderator awards the points, which are required in order to make a move forward. For each correct answer, a pin must be placed on the appropriate island. This scenario covers six topics that apply to everyday usage of the Internet. These are online shopping, gaming, information searches, social media, messaging and emails, and video platforms. "Security Surfer" provides a good basis for correct use of the Internet.

Fig. 11 Learning scenario "Security Surfer: Hazards and Protective Measures" in German (analog)—available in three levels of difficulty

6. SUMMARY AND FURTHER FOCUS

The article outlines how the objectives of the SecAware4school project were met: the individually defined measures have been effectively implemented based on examples from pilot schools, and sustainability within the

individual schools can also be achieved after the project ends. The project and the project team received strong positive feedback from the pilot schools, although it is not easy for the schools themselves to organize such a project internally. The project made it clear to everyone involved how important it is to establish "information security" in schools.

The understanding that information security is also of great importance for skills development in schools implies that appropriate teacher training needs to be put in place. Drossel & Eickelmann (2018) investigated the role of teacher professionalization in the implementation of new technologies in education. Their survey of the literature shows that on average it is relatively unusual—compared with international norms—for teachers in German schools to take part in external and internal professionalization programs focused on the use of digital media [9]. Their study of external measures shows that participation in courses designed to integrate IT into teaching and learning is comparatively rare in Germany.

Only about one in eight school principals, by their own account, encourage teachers to engage in further training in media education [11], while about one third require teachers to make digital media a fixture in their classroom practices [12]. This problem was also evident in the SecAware4school project, where some of the pilot schools were unable to find a teacher who was willing to complete the extensive training and certification process to become an information security officer—for the teachers it involves a considerable amount of extra work. The offer of free ICDL certification for pupils and teachers that the project made available was also not fully taken up. Nevertheless, the SecAware4school research project has succeeded in attracting a fair number of participants with the help of an ongoing campaign designed to convince people of its benefits.

The study [9] essentially revealed two types of teachers in Germany: the authors refer to the first type, representing the majority (about 85 percent), as "reluctant professionalizers." In this group, in particular, there is very little chance that the teachers will work together to improve the use of IT in the classroom, and the likelihood of them taking part in external training measures is less than 10 percent [9]. Only about 15 percent of teachers can be assigned to the second type, a group the authors call "committed professionalizers" [9]. A significantly higher proportion of this group will make regular use of computers in their classes: they tend to be much more confident about using computers and give their students far more encouragement in developing computer-related skills [9]. The sample in the study shows that the results of the second type are invariably higher than the German average, while the first type achieves results that are consistently below average. Overall, this study clearly confirms that external and internal professionalization measures in media studies are an important part of successfully implementing digital education in German schools [9].

However, IT and digital education are also a primary basis for information security issues. It should therefore come as no surprise that the SecAware4school project's objective—namely, to increase information security and foster an appropriate sense of awareness—had scarcely been touched upon in the pilot schools prior to the start of the project. Interesting game-based learning methods with a practical application to real situations and good best-practice examples with an ongoing impact on the pilot schools can also inspire other schools. With regular project days, new seminars, or freshly defined elective courses—incorporating self-creation and train-the-trainer concepts—this topic can be made an inspiring part of everyday school life and increase awareness of information security among pupils, teachers, and parents. The earlier awareness raising starts, the better, because our society will become smarter and increasingly digital in the future. Digitization must be connected with information security and information security with awareness.

7. ACKNOWLEDGMENTS

We are very grateful for input from the "Research Group Scholl" at TH Wildau in its 2019/2020 incarnation and would like to recognize the following individuals for their steadfast commitment: Denis Edich, Josephine Gerlach, Stefanie Gube, Peter Koppatz, and Frauke Prott. We are also grateful to the staff of the research group for their input over the past years. We would like to thank Dietmar Pokoyski (known_sense) for his imaginative support as a contractor in our projects.

8. REFERENCES

[1] E.O. Acquah, H.T. Katz, "Digital game-based L2 learning outcomes for primary through high-school students: A systematic literature review", **Computers & Education**, 143, 103667, 2020. https://www.sciencedirect.com/science/article/pii/S0360131519302209. Accessed February 25, 2020.

[2] BAköV, Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern, **Handbuch IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung**/Federal Academy of Public Administration in the Federal Ministry of the Interior, Manual IT Security Officer in Public Administration, Version 5.0, 2016.

[3] A. Bandura, **Social-learning theory of identificatory processses**, Handbook of socialization theory and research (213), 1969, p. 262.

[4] M. Beyer, S. Ahmed, K. Doerlemann, S. Arnell, S. Parkin, A. Sasse, N. Passingham, **Awareness is only**

the first step: A framework for progressive engagement of staff in cyber security, Hewlett Packard, Business white paper, 2016.

[5] BITCOM e.V., **Digitale Schule–Vernetztes Lernen, Ergebnisse repräsentativer Schüler- und Lehrerbefragung zum Einsatz digitaler Medien im Schulunterricht**, Berlin, 2015. https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2015/Studien/Digitale-SchulevernetztesLernen/BITKOM-Studie-Digitale-Schule-2015.pdf. Accessed February 25, 2020.

[6] Boyd, D., "Effective teaching in accelerated learning programs", **Adult Learning**, 15 (1-2), 2004, pp. 40-43.

[7] D. Bressler, A. Bodzin, "A Mixed Methods Assessment of Students' Flow Experiences During a Mobile Augmented Reality Science Game", **Journal of Computer Assisted Learning,** 29(6), 2013, pp. 505-517.

[8] Civey, "Die Digitalisierungsumfrage, Umfrageergebnisse und Zitate von Experten", 2019. https://assets.ctfassets.net/ublc0iceiwck/2Ixvr7MQMfRNJmvRlNwMEo/ecf9c854cc0f81f2cfe4266a3fa6e79/Digitalisierungsumfrage_TLGG_Civey_Ergebnisse.pdf. Civey. March 14, 2019. https://civey.com/newsroom/pressemitteilung/digitalisierungsstudie-gewaltiger-digitaler-nachholbedarf-bei-aerzten. Accessed October 17, 2019.

[9] K. Drossel, B. Eickelmann, "Die Rolle der Lehrerprofessionalisierung für die Implementierung neuer Technologien in den Unterricht–Eine Latent-Class-Analyse zur Identifikation von Lehrertypen", **MedienPädagogik: Zeitschrift für Theorie und Praxis der Medienbildung**, 31, 2018, pp. 166-191. https://www.medienpaed.com/article/view/487/609. Accessed February 25, 2020.

[10] X. Fang, J. Zhang, S. Chan, Development of an Instrument for Studying Flow in Computer Game Play. **International Journal of Human-Computer Interaction**, 29(7), 2013, pp. 456-47.

[11] J. Gerick, H. Schaumburg, J. Kahnert, B. Eickelmann, "Lehr- und Lernbedingungen des Erwerbs informationsbezogener Kompetenzen in den ICILS-2013-Teilnehmerländern". In **ICILS 2013 – Computer- und informationsbezogene Kompetenzen von Schülerinnen und Schülern in der 8. Jahrgangsstufe im internationalen Vergleich**, Wilfried Bos, Birgit Eickelmann, Julia Gerick, Frank Goldhammer, Heike Schaumburg, Knut Schwippert, Martin Senkbeil, Renate Schulz-Zander, und Heike Wendt (editors), Münster: Waxmann, 2014, pp. 147–196. https://www.waxmann.com/waxmann-buecher/?no_cache=1&tx_p2waxmann_pi2%5Bbuch%5D=BUC123858&tx_p2waxmann_pi2%5Baction%5D=show&tx_p2waxmann_pi2%5Bcontroller%5D=Buch&cHash=a90f94affa8c2634f0a2168282de4a99. Accessed February 25, 2020.

[12] J. Gerick, B. Eickelmann, K. Drossel, R. Lorenz, "Perspektiven von Schulleitungen auf neue Technologien in Schule und Unterricht". In **ICILS 2013 - Vertiefende Analysen zu computer- und informationsbezogenen Kompetenzen von Jugendlichen**, Birgit Eickelmann, Julia Gerick, Kerstin Drossel, und Wilfried Bos (editors), Münster: Waxmann, 2016, pp. 60–92.

[13] J. Hamari, D. J. Shernoff, E. Rowe, B. Coller, J. Asbell-Clarke, and T. Edwards, "Challenging games help students learn: An empirical study on engagement, flow and immersion in game-based learning", **Comput. Human Behav.**, vol. 54, 2016. pp. 170–179.

[14] M. Helisch, D. Pokoyski (editors), **Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung.** Wiesbaden: Vieweg+Teubner, 2009.

[15] K. M. Kapp, The Gamification of Learning and Instruction, **Game-Based Methods and Strategies for Training and Education**. San Francisco: Pfeiffer, 2012, pp. 10-12.

[16] K. M. Kapp, **Two Types of Gamification**, 2013. http://karlkapp.com/two-types-of-gamification. Accessed January 16, 2020.

[17] S. Linek, D. Albert, "Game-based Learning, Gender-specific Aspects of Parasocial Interaction and Identification", **International Technology, Education and Development Conference** (INTED), 2009.

[18] M. Mataric, "Reward functions for accelerated learning", **Machine Learning Proceedings** 1994, pp.181-189.

[19] S. Pereira, J. Fillol, P. Moura, "Young people learning from digital media outside of school: The informal meets the formal", Comunicar, **Media Education Research Journal**, 27(1), 2019. https://www.scipedia.com/public/Pereira_et_al_2019a. Accessed February 25, 2020.

[20] C. Rose, M. Nicholl, "Accelerated learning for the 21st century", **The six-step plan to unlock your master-mind**, Dell Books, 1998.

[21] M. Scholl, F. Fuhrmann, D. Pokoyski, "Information security awareness 3.0 for job beginners", J.E. Varajão, M.M. Cruz-Cunha, R. Martinho, R. Rijo, N. Bjørn-Andersen, R. Turner, D. Alves, **Proceedings of the Conference on ENTERprise Information Systems**, 2016, pp. 433-436.

[22] H. Stuart, E. Lavoué, A. Serna, J.C. Marty, **Structural Gamification for Adaptation based on**

Learning Analytics, EARLY, Aachen, Germany. Aug 2019, pp. 383.

[23] J. Trybus, **Game-Based Learning. What it is, Why it Works, and Where it's Going**. New Media Institute, 2014. http://newmedia.org/game-based-learning--what-it-is-why-it-works-and-where-its-going.html. Accessed June 28, 2017.