2019 LiCE London International Conference on Education

Technische Hochschule Wildau [FH] *Technical University of Applied Sciences*

M. Scholl, R. Schuktomow, P. Koppatz, S. Gube

SecAware4school: Information Security Awareness (ISA) in Everyday School Life

Raising ISA through Gamification

Outline

1. Introduction
2. Background: Information security awareness (ISA) in everyday school life
3. Survey and participative dialogues to identify issues
4. Content summary and review of current activities
5. Outlook

1. Introduction: Core values & safeguards

Digitization and information technologies are all-pervasive.

At the same time, the risk of sensitive data being misused is increasing.

The core values inherent to **information security (IS)** are [BA16]:

Confidentiality

Integrity

Availability

Further safeguards include ***authenticity*** and ***non-repudiation***.

1. Introduction: GBL, AccL & AL

The Game-Based Learning, Accelerated Learning, and Authentic Learning approaches are combined in order to achieve the stated goals.

Game-Based Learning (GBL):

GBL motivates and enables students to look at a set goal and provide direct feedback [Li09] [Fa13].

Accelerated Learning (AccL):

AccL challenges students to go beyond passive perception and actively create knowledge [Ba69] [Ma94] [Ro98] [Bo04].

Authentic Learning (AuL):

AuL focuses on the application of knowledge in real contexts and situations. The central aspect here is learning from experience, from real or simulated problems [Sc16].

2. ISA in everyday school life

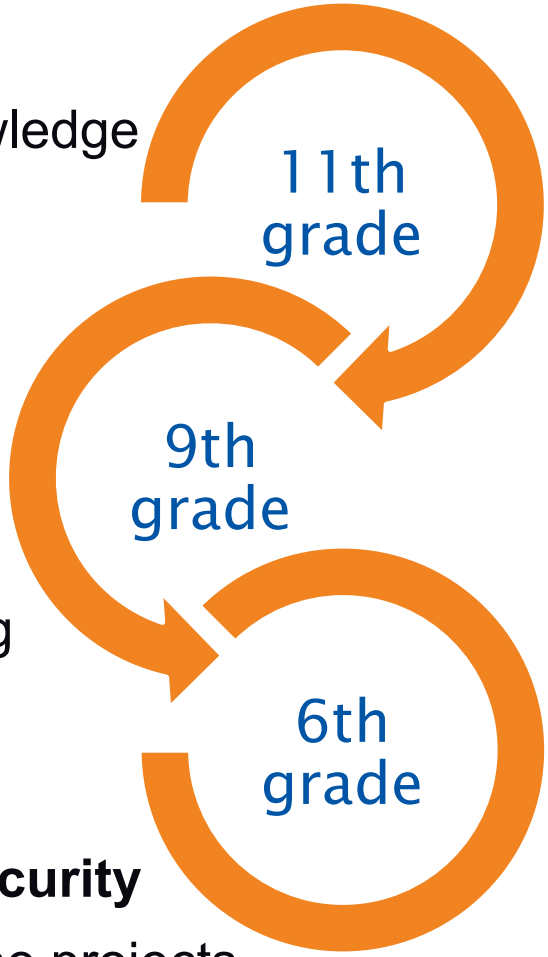
As users of Internet services and social networks, young people should be introduced to the careful handling of sensitive data in a playful way and develop their digital competence and technical understanding in the same way.

Ultimately, the pupils should be self-reliant and capable of operating in the digitized world in a conscious manner by:

- independently recognizing potential dangers on the Internet
- assessing risks
- taking preventive protective measures

2. ISA in everyday school life

Experience should not be limited to the individual; instead it should lead to a closed loop in which knowledge is transferred and maintained among pupils.



While younger pupils benefit in this way from the experience of older pupils, the older consolidate their knowledge by subsequently providing independent moderation and support for the learning scenarios in their school.

The qualification of the pupils as so-called **youth security advisors** is thus another important cornerstone of the projects.

3. Survey & participative dialogues

An anonymous online survey was conducted for 4–5 pilot schools in Berlin/ Brandenburg using ***LamaPoll*** from September 28 to December 3, 2018.

Altogether the survey was accessed 1,821 times:
it was filled out 827 times and completely filled out 710 times.

Not all the questions in the online system were mandatory, so some questions could be skipped.
As a result, some questions have a higher number of answers than others.

Moreover, so-called creative workshops were set up to involve pupils and teachers from the very beginning in developing the games and background stories of the learning scenarios.

3. Survey & participative dialogues

Our survey consisted of a total of nine questions.
The first questions were used to collect demographic data from the participating schools.

Further question were:

- *A warm-up question about secure passwords*
- *“Do you know how you can protect your own private sphere online?”*
- *“How often do you use images from the Internet—e.g., for presentations?”*
- *“Have you ever been the victim of data theft (e.g., your log-in data was stolen)?”*
- *“To what extent are you interested in the following topics?”*
- *“What other topics are you interested in?”*

3. Survey & participative dialogues: Results

The main topics for the pilot schools are:

- **Information security** in general
- **Smartphone** settings
- Secure use of **social networks**
- **Privacy** protection
- **Encryption** as a security aspect
- Types and modes of action of harmful software (**Malware**)
- **Programming** (what do crackers/hackers do …)
- **Data protection** in general

3. Survey & participative dialogues: Results

The topic ***fake news*** is of similar interest to all respondents from the pilot schools.

In corporate awareness research, this online phenomenon has also become an ongoing issue, but its significance for the economy and the company's own working environment is **still largely underestimated** [Ma18].

Disinformation is not a consequence of digital overload and it is not enough simply to check the source of information [Ta18] [Ma18].

It is important to understand the principle of false reporting in context. A sensitization measure must take this into account: **self-reflection** and **digital prudence** [Ma18].

4. Content summary

For the research project “SecAware4school” various phases were defined For three different grades in cyclical rather than classical terms.

The **survey** in the initial phase related to the interests of all the target groups involved.

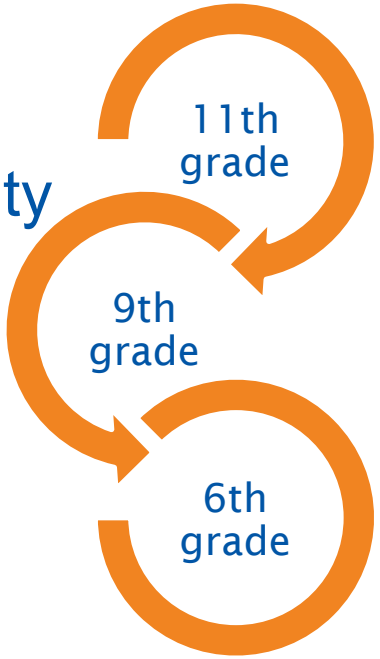
In a further step, the **information events** were intended to offer details about the project to the classes that would actively participate in the development of experience-oriented learning scenarios and awareness trainings. This proved to be a **very time-intensive** activity.

Creative workshops were the starting point for participative brainstorming and scenario development. The actual task of **game development** was left to the project team and then **tested** in the schools.

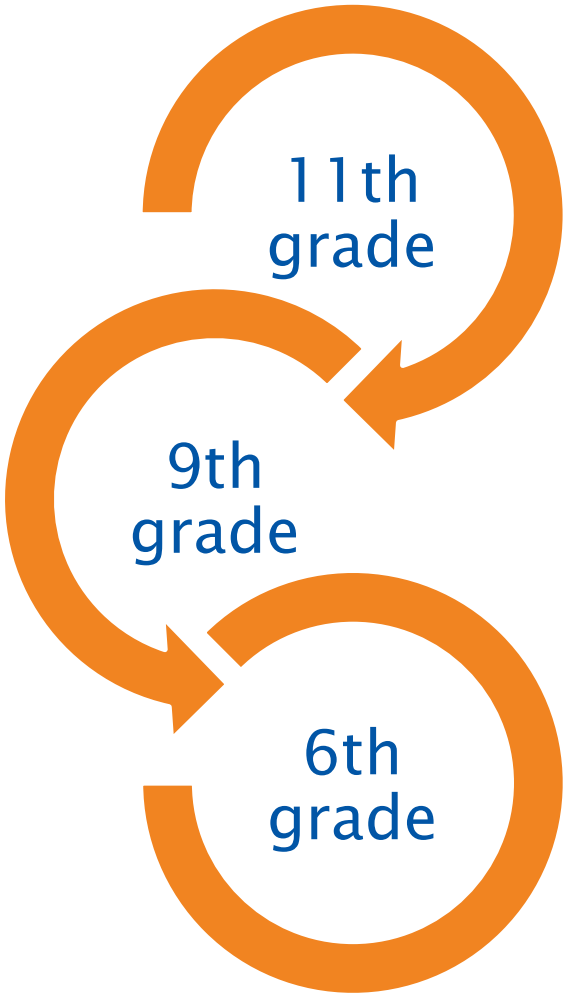
The Project SecAware4school

The **SecAware4school project** includes lower (6th), middle (9th) and higher (11th) grades, developing a total of 10 learning scenarios at three different levels of difficulty for a total of 30 analogue and digital learning scenarios:

- Learning scenarios at three levels of difficulty
- Security issues in the real world
- Young security advisors for the younger school students
- Teachers as information security officers.

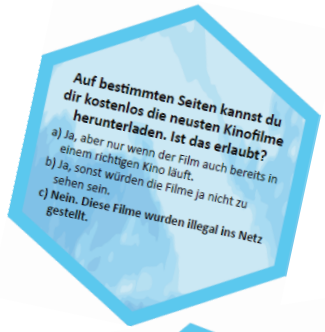


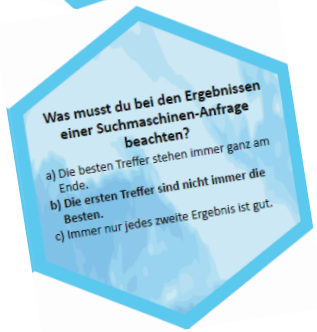
Hazards & protective measures (analogue)



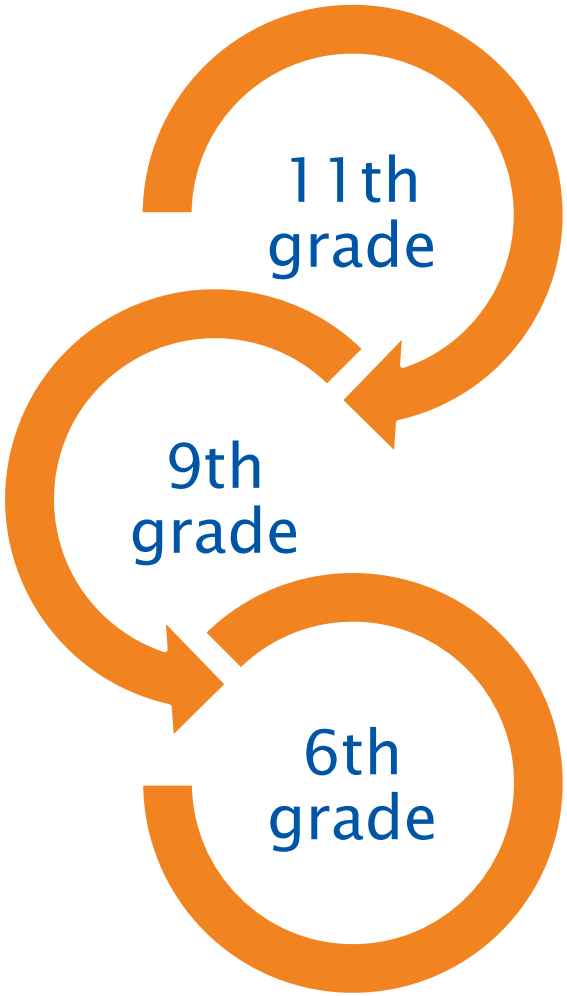
Objective of the learning scenario:
Knowledge of threats and safeguards for information security
Expansion of knowledge of information security

Task:
Strategy Game. Explain and guess important information security terms. Identify hazards and information security measures.





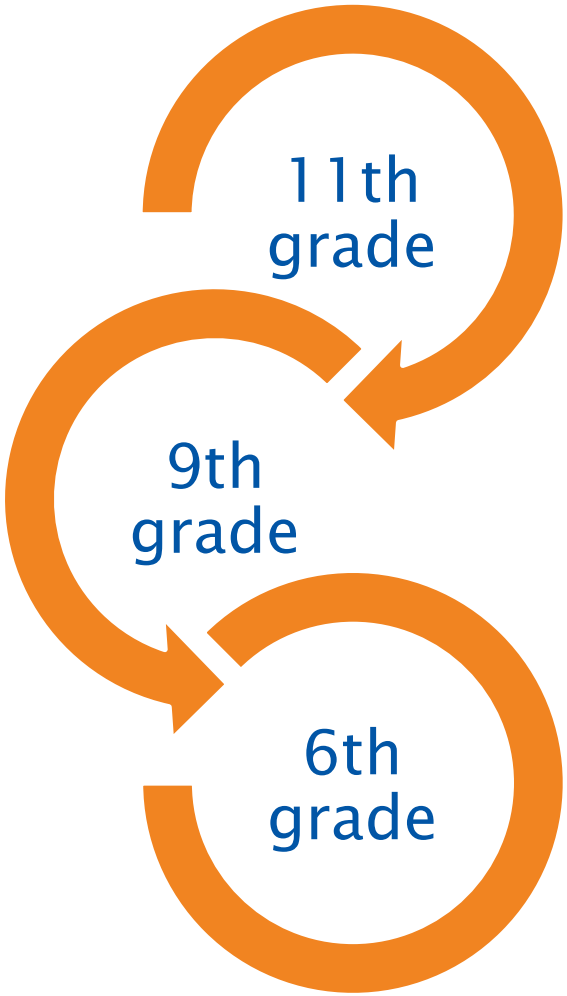
Recognize the internet norms
(analogue)



Objective of the learning scenario:
Learning and repeating of rules of conduct on the Internet.
Changing behavior based on list of dos and don’ts.

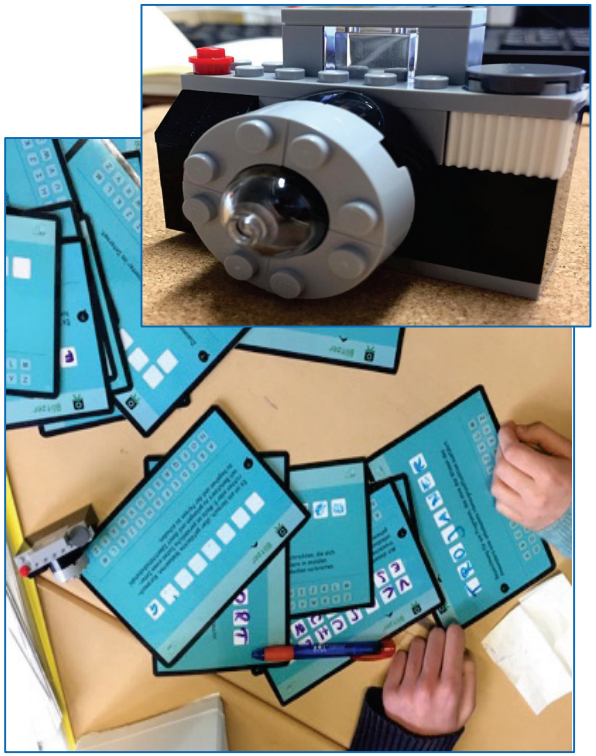
Task:
Hints and rules from the puzzle to remember.

Rapid Guessing
(analogue + digital)

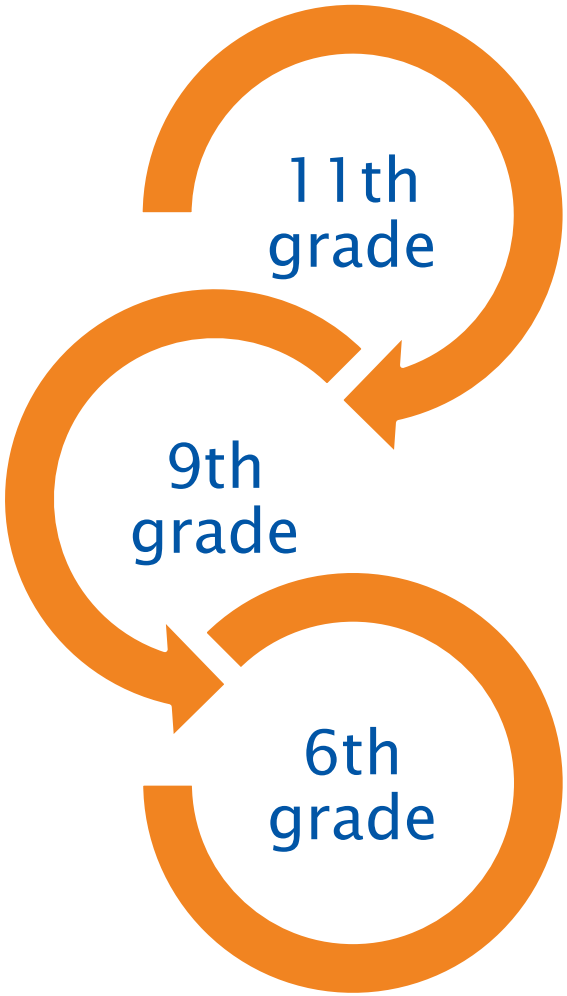


Objective of the learning scenario:
Learning important terms and their meaning.

Task:
Guess important information security terms with discussion.



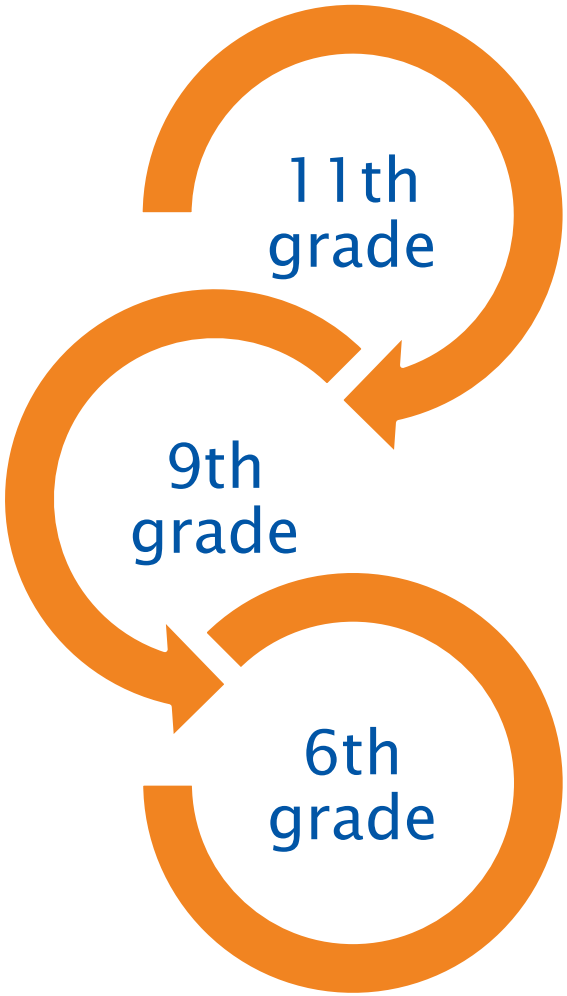
Rights in photos
(digital)



Objective of the learning scenario:
Knowledge and ability to assess current security incidents concerning image rights. Sensitization to the use of images.

Task:
Evaluate the usability of image rights according to GDPR.

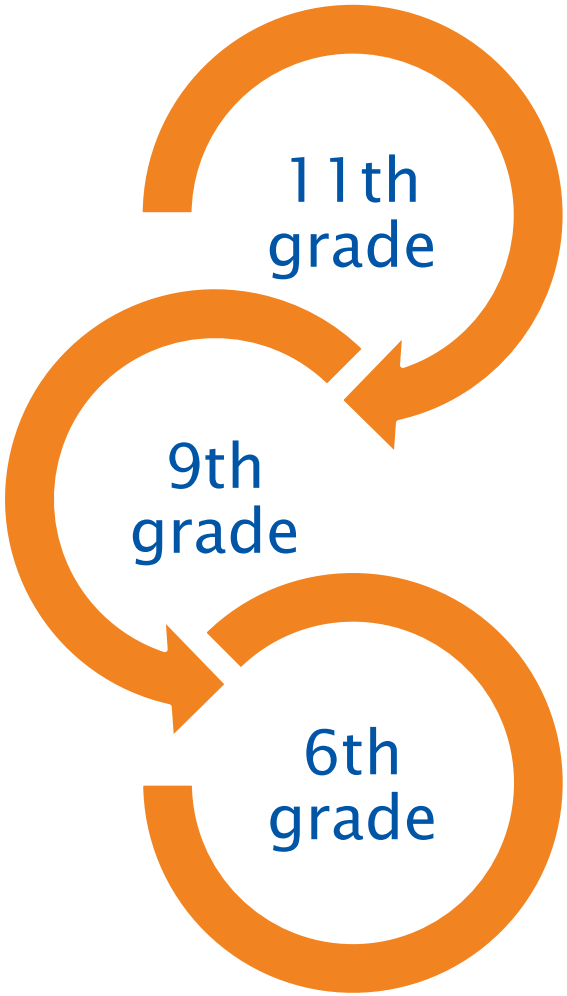
Storytelling in IS
(analogue + digital)



Objective of the learning scenario:
Repetition and deepening of information security knowledge and technical terms.

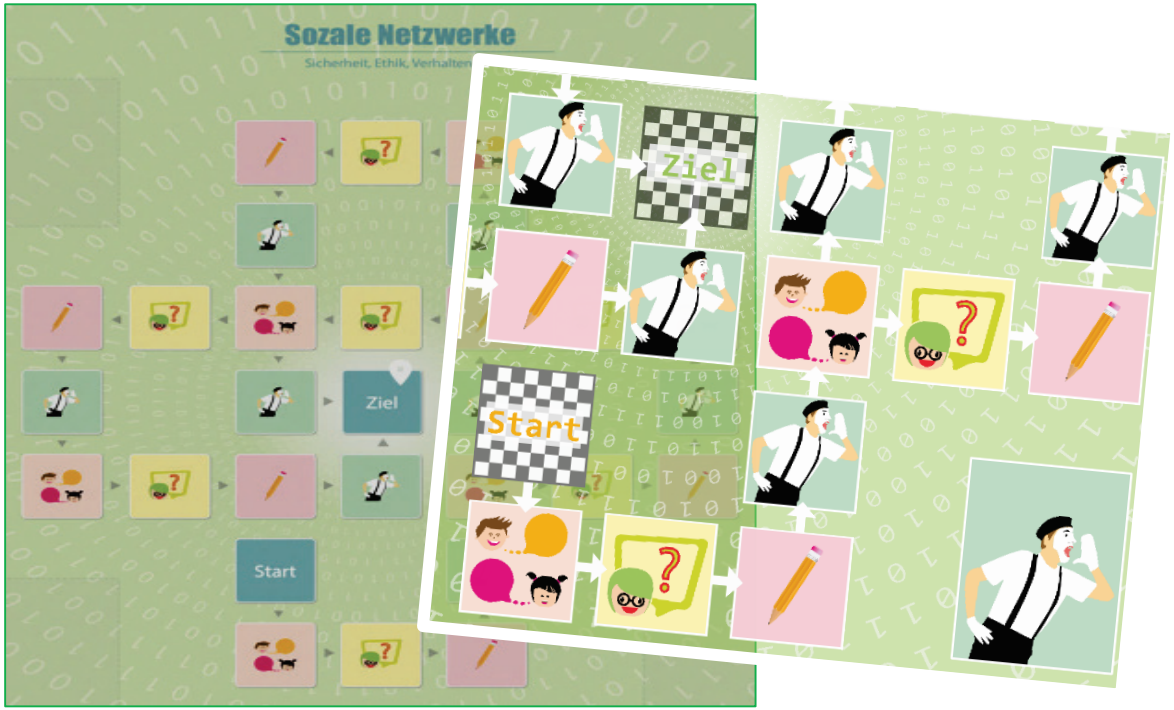
Task:
Use random symbols to write down a realistic story of information security using important and real technical terms.

Behavior in social networks
(analogue)

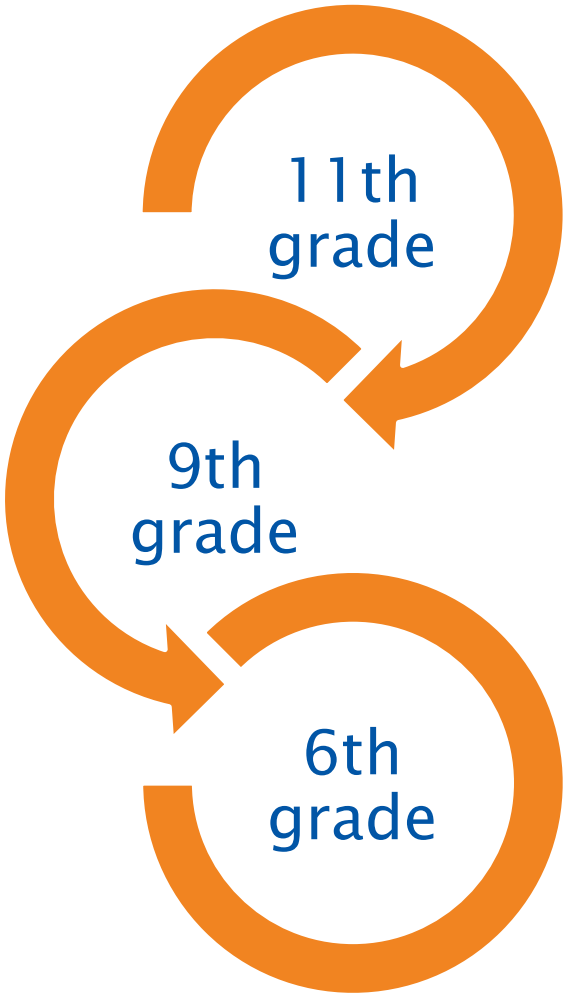


Objective of the learning scenario:
Awareness of safe security behavior in social networks.

Task:
Interactive educational game explaining and guessing certain information security terms in social networks.

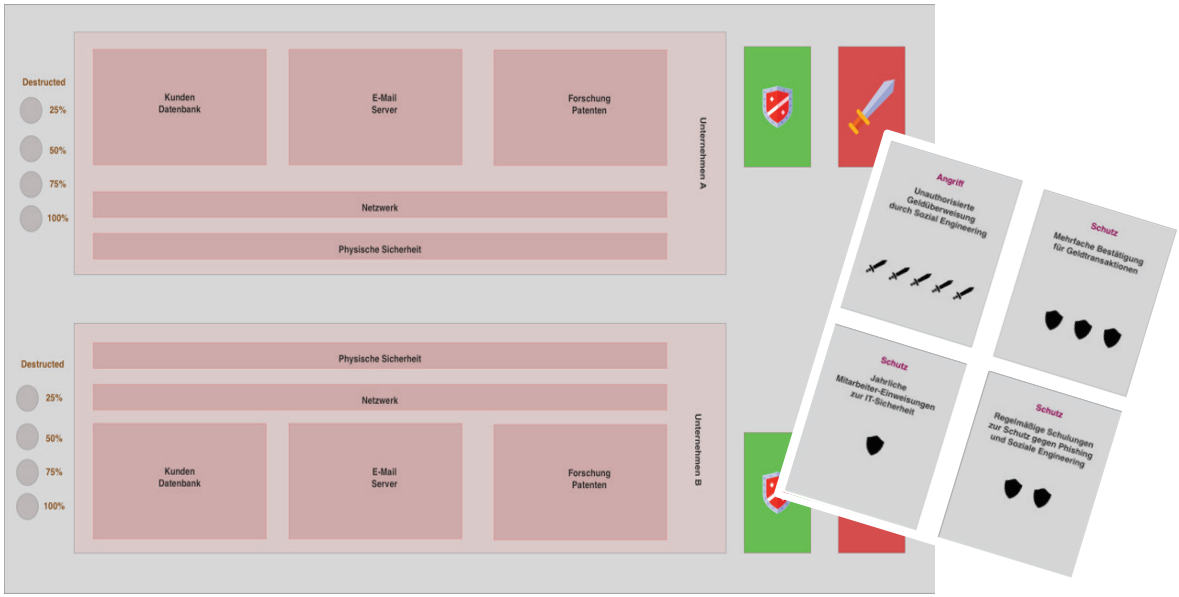


Security duell in job situations
(analogue)

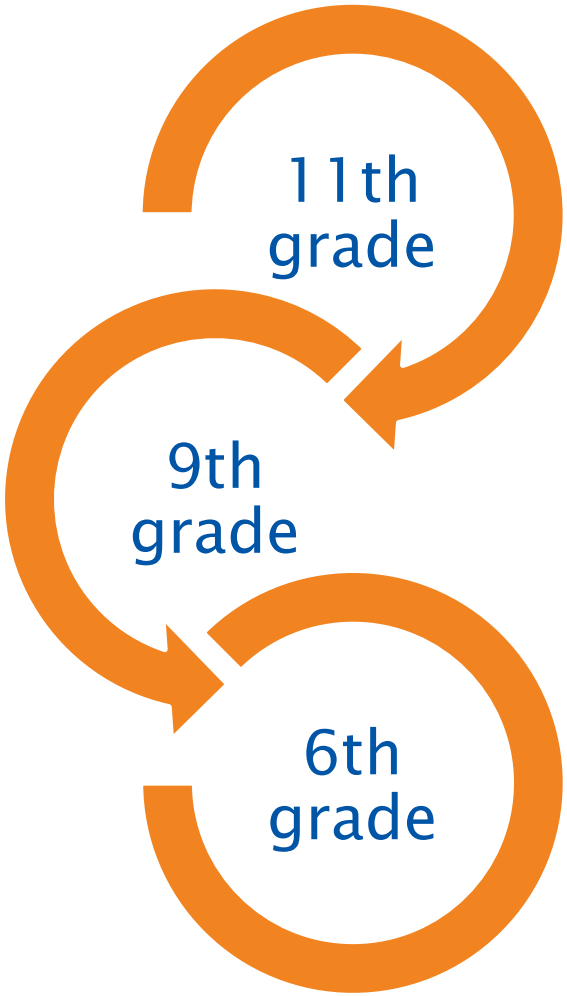


Objective of the learning scenario:
Information on security-relevant decision situations, possible security gaps, consequences and protective measures.

Task:
Interactive educational game to protect and attack sensitive data. Make decisions in the area of private and work-related information security.



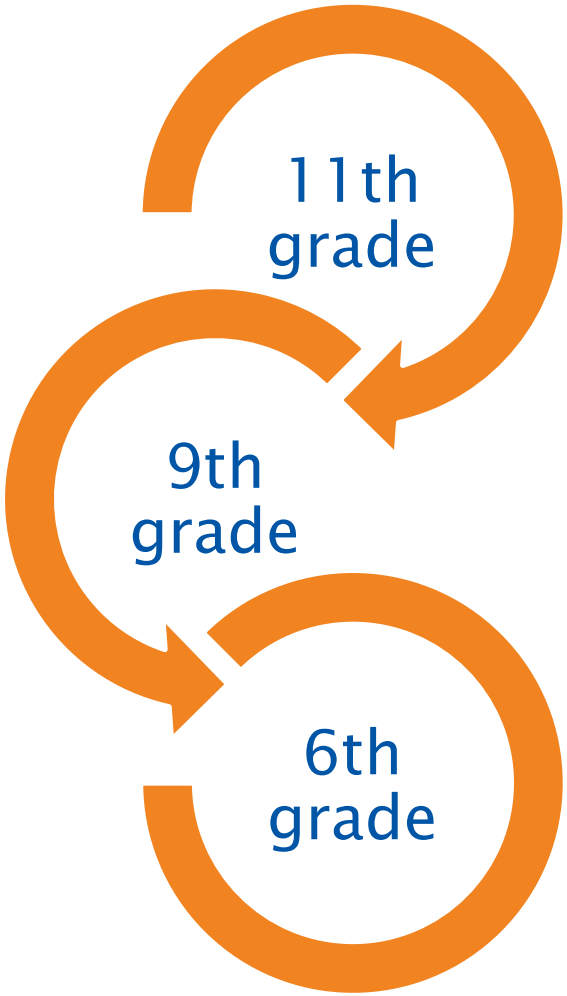
Fake news
(analogue + digital)



Objective of the learning scenario:
Sensitization to information collection and manipulation.

Task:
Identify fake messages based on examples.

Clear Room: Data Espionage (digital)



Objective of the learning scenario:
Sensitize the safekeeping of sensitive information at work, at school or at home.

Task of the learning scenario:
Which objects should be enclosed / removed when leaving the room?

5. Outlook

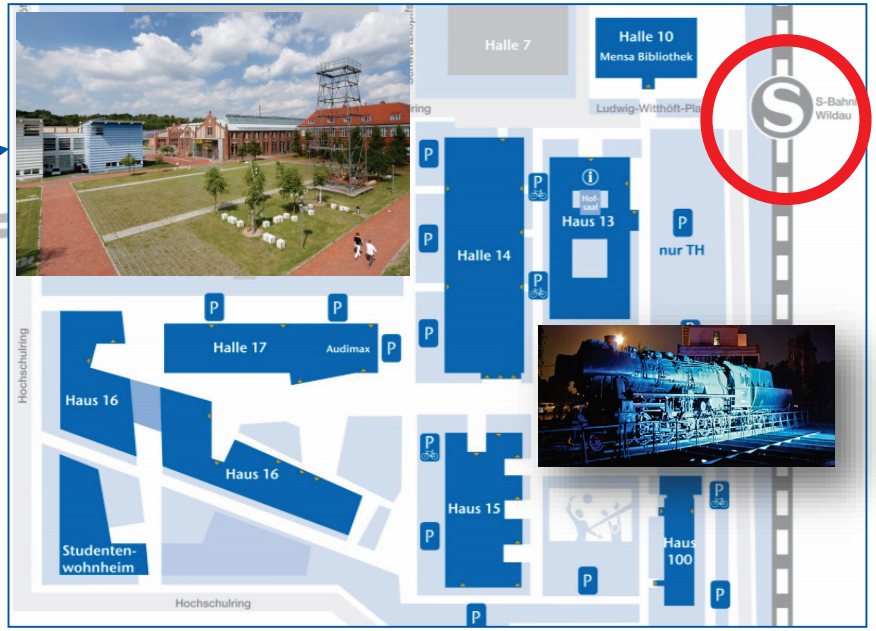
The project will end on August 31, 2020.

All ten experience-based learning scenarios in three different levels can be borrowed by schools.

Digital game versions will be usable from the website.
https://secaware4school.wildau.biz

- **Pupils** will be trained as security advisors and will be able to complete the ECDL “IT Security” certification.
- **Teachers** can also do ECDL certification; one teacher from each pilot school will become an information security officer.
- Knowledge will be passed on through **parents**’ evenings and social interaction.

Where is the TUAS Wildau located?



References

[BA16] BAköV, Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern (Hrsg.): Handbuch IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung, Version 5.0, 2016.

[Ba69] Bandura, A.: Social-learning theory of identificatory processes. Handbook of socialization theory and research (213), S. 262, 1969.

[Be16] Beyer, M.; Ahmed, S.; Doerlemann, K.; Arnell, S.; Parkin, S.; Sasse, A.; Passingham, N.: Awareness is only the first step. A framework for progressive engagement of staff in cyber security, Hewlett Packard, Business white paper, 2016
.

[Bo04] Boyd, D.: Effective teaching in accelerated learning programs. Adult Learning, 15 (1-2), S. 40-43, 2004.

[Br13] Bressler, D.; Bodzin, A.: A Mixed Methods Assessment of Students' Flow Experiences During a Mobile Augmented Reality Science Game. Journal of Computer Assisted Learning, 29(6), S. 505-517, 2013.

References

[Co17] Codish, D.; Ravid, G.: Gender Moderation in Gamification: Does One Size Fit All?. Proceedings of the 50th Hawaii International Conference on System Sciences, S. 2006-2015, 2017.

[Da06] Dark, M.J.: Security Education, Training and Awareness from a Human Performance Technology Point of View. In (Whitman, M.E.¸Mattord, H.J. Hrsg.): Readings and Cases in Management of Information Security, Course Technology, Mason, S. 86-104, 2006.

[Fa13] Fang, X.; Zhang, J.; Chan, S.: Development of an Instrument for Studying Flow in Computer Game Play. International Journal of Human-Computer Interaction, 29(7), S. 456-47, 2013.

[Ha18] Haucke, A.; Pokoyski, D.: Mea culpa - Schuld, Scham und Opferrolle bei Social Engineering. kes, 1, S. 6-8. 2018.

[He09] Helisch, M.; Pokoyski, D. (Hrsg.): Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung. Wiesbaden, Vieweg + Teubner, 2009.

References

[Hu16] Huotari, K.; Hamari, J.: A Definition for Gamification: Anchoring Gamification in the Service Marketing Literature. Electronic Markets, 27 (1), S. 21-31, 2016.

[Ki14] Kim, E.B.: Recommendations for information security awareness training for college students, Information Management & Computer Security, 22 (1), S. 115-126, 2014.

[Li09] Linek, S.; Albert, D.: Game-based Learning: Gender-specific Aspects of Parasocial Interaction and Identification. International Technology, Education and Development Conference (INTED), 2009.

[Ma18] Matas I.; Pkoyski D.: Von der Ente zur End-Täuschung. Kes 5, S. 19-23, Oktober 2018.

[Ma94] Mataric, M.: Reward functions for accelerated learning. Machine Learning Proceedings 1994, S. 181-189, 1994.

References

[Po09] Pokoyski, D.: Security Awareness: Von der Oldschool in die Next Generation – eine Einführung. In (Helisch, M.; Pokoyski, D. Hrsg.): Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung, Wiesbaden, Vieweg+Teubner, S. 1-8, 2009.

[Ro98] Rose, C.; Nicholl, M.: Accelerated learning for the 21st century: The six-step plan to unlock your master-mind. Dell Books, 1998.

[Sc16] Scholl, M.; Fuhrmann, F.; Pokoyski, D.: Information security awareness 3.0 for job beginners. In: (Varajão, J.E.; Cruz-Cunha, M.M.; Martinho, R.; Rijo, R.; Bjørn-Andersen, N.; Turner, R.; Alves, D. (Hrsg.): Proceedings of the Conference on ENTERprise Information Systems, S. 433-436, 2016.

[Si13] Singh, A.N.; Picot, A.; Kranz, J.; Cupta, M.P.; Ojha, A.: Information security management (ism) practices: Lessons from select cases from India and Germany, Global Journal of Flexible Systems Management, 14 (4), S. 225-239, 2013.

References

[Si17] Silic, M.; Back, A.: Impact of Gamification on User's Knowledge-Sharing Practices: Relationships between Work Motivation, Performance Expectancy and Work Engagement. Proceedings of the 50th Hawaii International Conference on System Sciences, S. 1308-1317, 2017.

[St13] Styles M.: Constructing Positive Influences for User Security Decisions to Counter Corporate or State Sponsored Computer Espionage Threats. In: (Marinos L.; Askoxylakis, I. Hrsg.): HAS 2013, Lecture Notes in Computer Science, Vol. 8030. Berlin/Heidelberg, Springer, S. 197-206, 2013.

[Ta18] TAKE AWARE EVENTS (Hrsg.): Von der Ente zur End-Täuschung. Studie, veröffentlicht anlässlich der 2. Social Engineering-Konferenz BLUFF CITY 2018 in Köln, 2018.

[Wo07] Workman, M.: Gaining Access with Social Engineering: An Empirical Study of the Threat, Information Systems Security, 16 (6), S. 315-331, 2007.

Technische Hochschule Wildau [FH]
Technical University of Applied Sciences

Thank you for your attention! Q & C ?

Contact:
Prof. Dr. Margit Scholl
margit.scholl@th-wildau.de
https://www.th-wildau.de/scholl